Glossario Bitcoin

Bitcoin Italia Network

2025-04-17

Descrizione

Il glossario sui più comuni termini Bitcoin e criptovalute

0-conf

Acronimo di: zeroconf o zero confirmation

Livello: intermedio

Argomento: tecnologia

0-conf, Zero-conf, scritto anche senza separatore in 0conf, indica una transazione che non ha ancora ricevuto alcuna conferma.

È lo stato in cui si trova la transazione prima di essere inclusa in un blocco, e viene chiamata anche transazione non confermata.

La possibilità di sostituire una transazione non confermata può essere anche esplicitata dall'utente quando crea la transazione impostandola in modo esplicito tramite l'opzione RBF.

Generalmente fintanto che la transazione si trova in questo stato, si consiglia non considerarla come sicura, perché potrebbe essere sostituita da un'altra transazione, operazione chiamata Transaction Replacement, ma considerato che i tempi di conferma possono essere anche molto lunghi, sia per l'incertezza dei tempi di creazione di un nuovo blocco che mediamemente sarebbero 10 minuti ma a volte possono essere anche superiori ad un ora, ci sono dei casi nei quali può valer la pena correre il rischio e accettare come valida una transazione 0-conf.

Perché le transazioni non confermate vengono considerate non sicure?
Le transazioni Bitcoin vengono trasmesse attraverso un sistema distribuito asincrono in cui non esiste un "primo" a livello globale che riceve la transazione. Quello che Alice ha visto per prima, Bob potrebbe vederlo per secondo. Il design di Bitcoin non prevede un meccanismo che consenta ad Alice e Bob di accordarsi su quale transazione sia stata realmente la prima; tutto ciò che possono fare è

aspettare di vedere quale di queste transazioni viene confermata in un blocco valido della migliore catena di blocchi.

Gli aggressori esperti del Double Spend utilizzano strumenti per mappare la connettività della rete, effettuando spese innocue che sembrano in conflitto e vedendo quali versioni appaiono presso quali merchant e in quali blocchi. In questo modo possono creare due versioni della stessa transazione, una da inviare alla vittima e una da inviare ai miner per la conferma.

La presenza del pagamento non sostituibile al merchant impedisce al suo nodo di venire a conoscenza di una doppia spesa fino a quando non compare in un blocco minato da un miner che stava semplicemente minando la transazione che ha visto per prima. Questo schema semplice e comune viene a volte ulteriormente amplificato da altre tecniche, come l'utilizzo di catene di transazioni non confermate, fee basse o transazioni non standard.

Di conseguenza, la stragrande maggioranza della sicurezza delle transazioni non confermate non proviene dal sistema Bitcoin, ma da fattori esterni come il gran numero di utenti Bitcoin onesti che non cercherebbero mai di frodare i loro venditori, la tolleranza tra i venditori per piccole quantità di frodi, la capacità (o la minaccia) dei venditori di ricorrere al sistema legale o ad altri tipi di ricorso e altri fattori che non hanno nulla a che fare con la progettazione del protocollo Bitcoin.

Tutte queste cose valgono anche per la RBF opt-in (e non sono diverse dalla situazione dei pagamenti con carta di credito negli Stati Uniti, che sono facilmente stornabili per mesi dopo lo scambio e che tuttavia hanno tassi di frode abbastanza bassi da essere accettati da quasi tutti i merchant importanti). Inoltre, poiché la RBF può talvolta eliminare i lunghi tempi di conferma, alcuni merchant che in precedenza si sentivano costretti ad accettare transazioni non confermate per evitare spiacevoli ritardi potrebbero non aver più bisogno di farlo, riducendo così la loro esposizione alle frodi.

Job Declarator

Livello: avanzato

Argomento: tecnologia

Stratum v2 rappresenta un'evoluzione significativa nel protocollo di comunicazione per il mining di Bitcoin in pool, progettato per superare le limitazioni della sua precedente versione, Stratum v1 . Questo nuovo protocollo funge da ponte di comunicazione tra i minatori e le mining pool, con l'obiettivo primario di migliorare la sicurezza, l'efficienza e, soprattutto, la decentralizzazione del processo di mining . Tra i miglioramenti chiave introdotti da Stratum v2 spiccano una maggiore sicurezza attraverso la crittografia delle comunicazioni, una maggiore efficienza grazie alla trasmissione di dati in formato binario, e una più ampia autonomia per i minatori nella selezione delle transazioni da includere nei blocchi . L'intento è quello di rendere il mining in pool più simile al

mining solitario per quanto riguarda il controllo sui set di transazioni . Per raggiungere questi obiettivi, Stratum v2 introduce diverse nuove sub-protocolli . L'evoluzione da Stratum v1 a v2 riflette una crescente necessità di un ecosistema di mining più sicuro, efficiente e decentralizzato. L'introduzione della selezione delle transazioni controllata dai minatori rappresenta un cambio di paradigma fondamentale, spostando il potere decisionale precedentemente centralizzato nelle mani delle pool verso i singoli partecipanti .

Nel contesto di Stratum v2, il termine "job" si riferisce a un'unità di lavoro assegnata ai minatori, contenente tutte le informazioni necessarie per eseguire l'hashing su un'intestazione di blocco candidata . Le mining pool distribuiscono questi "mining job" ai singoli minatori, indipendentemente dalle loro capacità hardware . Stratum v2 definisce principalmente due tipi di job: lo Standard Job e l'Extended Job . Gli Standard Job sono destinati all'header-only mining (HOM) con Merkle Root fissi, mentre gli Extended Job consentono Merkle Root variabili . Con l'introduzione del Job Declaration Protocol, sono stati introdotti anche i Custom Job, che permettono ai minatori di scegliere i propri set di transazioni . Il concetto di "job" ha quindi subito un'evoluzione in Stratum v2 per accogliere una maggiore autonomia da parte dei minatori riguardo al contenuto dei blocchi su cui lavorano, superando il modello di Stratum v1 incentrato sulle pool . In Stratum v1, i job erano interamente decisi dalla pool. L'introduzione dei "Custom Job" in Stratum v2, e i meccanismi per proporli e dichiararli, indicano un passaggio verso un processo di mining più collaborativo e meno gerarchico.

Il Job Negotiator è un componente cruciale di Stratum v2 che consente ai minatori di influenzare i set di transazioni inclusi nei blocchi che minano . Questa funzionalità innovativa permette ai minatori di costruire i propri template di blocco e di proporli alla pool per l'approvazione . Questo processo è parte del Job Negotiation Protocol . Il Job Negotiator opera come un sub-protocollo responsabile della distribuzione dei template dei minatori alla pool . In sostanza, i minatori possono negoziare con una pool un template di blocco, incluso il set di transazioni . Questa capacità rappresenta un cambiamento fondamentale nelle dinamiche di potere del mining in pool, offrendo ai minatori un maggiore controllo sull'inclusione delle transazioni e migliorando la resistenza alla censura .

L'interazione tra il minatore e la pool attraverso il Job Negotiator prevede uno scambio di messaggi strutturato. Sebbene non esista un "Job Negotiator Protocol" formalmente definito nella documentazione, si possono identificare i messaggi chiave coinvolti. Il minatore, attraverso il suo Job Negotiator, richiede innanzitutto un token per poter proporre un lavoro, utilizzando il messaggio AllocateMiningJobToken . La pool risponde con un AllocateMiningJobToken.Success, fornendo il token necessario per le successive fasi della negoziazione . Questo scambio iniziale indica un processo gestito per autorizzare i minatori a partecipare alla negoziazione dei job, prevenendo invii incontrollati. Una volta ottenuto il token, il minatore, spesso in coordinamento con un Tem-

plate Provider (che può essere un nodo Bitcoin locale), costruisce un template di blocco con le transazioni desiderate. Il Template Provider, come un nodo Bitcoin locale gestito dal minatore, fornisce i dati delle transazioni, che il Job Negotiator utilizza poi per costruire la proposta di job per la pool . Questa proposta viene inviata alla pool tramite il messaggio CommitMiningJob . Nella sua attuale implementazione di riferimento (SRI), la pool è tenuta a rispondere con un messaggio CommitMiningJob.Success, accettando la proposta del minatore . Questo impone alla pool di accettare le transazioni suggerite dal minatore, sottolineando l'enfasi sull'autonomia del minatore nella fase iniziale di implementazione di questa funzionalità. Tuttavia, sono previsti aggiornamenti futuri che includeranno meccanismi di fallback per i minatori nel caso in cui la pool dovesse rifiutare le loro proposte . Questo permetterà ai minatori di passare a un'altra pool o di minare in solitario se le loro selezioni di transazioni venissero costantemente rifiutate, rafforzando ulteriormente la resistenza alla censura. L'intero flusso di interazione, descritto come la "JN dance", evidenzia la connessione iniziale, la richiesta e l'allocazione del token, la consegna del template dal Template Provider, la proposta del job e la sua accettazione .

Il Job Declarator è un altro ruolo fondamentale in Stratum v2, coinvolto nella dichiarazione di template di blocco personalizzati dai minatori alla pool . Opera all'interno del Job Declaration Protocol . L'obiettivo principale del Job Declarator è impedire che le pool impongano unilateralmente il lavoro ai minatori . Questo protocollo prevede due ruoli distinti: il Job Declarator Client (JDC) lato minatore e il Job Declarator Server (JDS) lato pool . Il JDC riceve i template dal Template Provider e dichiara i job personalizzati al JDS . Il JDS, a sua volta, alloca token al JDC per la dichiarazione di job personalizzati e ne riconosce l'avvenuta dichiarazione .

Il Job Declaration Protocol prevede una serie di messaggi ben definiti per coordinare la creazione di lavoro personalizzato . Il JDC inizia richiedendo un identificatore per un futuro job di mining al JDS tramite il messaggio AllocateMiningJobToken . Il JDS risponde con successo con AllocateMiningJobToken.Success, fornendo un token che autorizza il client a dichiarare un job di mining . Successivamente, il JDC propone un set selezionato di transazioni al JDS per la creazione di un lavoro personalizzato attraverso il messaggio DeclareMiningJob . Il JDS riconosce l'avvenuta dichiarazione con DeclareMiningJob.Success o segnala un rifiuto con DeclareMiningJob.Error . In caso di collisioni negli ID brevi delle transazioni o se il JDS non riesce a ricostruire l'hash della lista completa delle transazioni, invia un messaggio IdentifyTransactions al JDC, che risponde con IdentifyTransactions.Success fornendo gli hash completi delle transazioni . Se il JDS rileva transazioni mancanti nel messaggio DeclareMiningJob, richiede i dati completi tramite ProvideMissingTransactions, a cui il JDC risponde con ProvideMissingTransactions.Success inviando le transazioni richieste . Infine, una volta trovato un blocco valido, il JDC lo invia al JDS tramite il messaggio SubmitSolution . Questo flusso di messaggi indica un processo strutturato che garantisce la coerenza tra il template proposto dal minatore e la visione della pool, in particolare riguardo al mempool

delle transazioni. Il JDC ha anche la responsabilità di implementare strategie di fallback, come il passaggio ad altre pool o il mining solitario, nel caso in cui il JDS rifiuti le dichiarazioni di job o le share, incentivando l'onestà da parte della pool . Questa separazione del Job Declaration Protocol dal Mining Protocol principale permette alle pool di gestire le connessioni di dichiarazione in modo indipendente dalle connessioni di mining (invio di share), migliorando la robustezza e l'efficienza del sistema complessivo .

Nelle prime versioni di Stratum V2, il "Job Negotiator" era un sottoprotocollo che permetteva ai miner di negoziare con i pool la selezione delle transazioni da includere nel blocco. Il termine "Negotiator" è stato sostituito con "Declarator" per sottolineare che i miner dichiarano unilateralmente i propri template, senza una negoziazione bidirezionale. La modifica rispondeva a feedback della community per chiarire il funzionamento unidirezionale.

DER

Acronimo di: Distinguished Encoding Rules

Livello: avanzato

Argomento: tecnologia

Le Distinguished Encoding Rules (DER) sono un formato di codifica utilizzato per serializzare dati strutturati, come le firme digitali. In particolare, il formato DER è una variante delle regole ASN.1 che fornisce una sintassi di trasferimento non ambigua per i dati strutturati.

DER funziona seguendo delle regole precise:

- **Definizione dei tipi di dati**: stabilisce come rappresentare diversi tipi di informazioni, come numeri, testi o date.
- **Struttura dei dati**: indica come organizzare le informazioni in sequenze, insiemi o altri formati.
- **Codifica dei valori**: specifica come trasformare i valori dei dati in una serie di numeri o simboli.
- **Regole di impacchettamento**: definisce come combinare i diversi elementi codificati in un unico insieme di dati.

In Bitcoin, DER viene utilizzato principalmente per codificare le transazioni e le firme digitali. Le firme ECDSA sono codificate utilizzando il formato DER. Una firma ECDSA è composta da due numeri: r e s. Questi vengono codificati in un flusso di byte usando il formato DER.
Il processo di codifica include:

- Inizio con il byte 0x30 che indica una struttura composta, che indica l'inizio della struttura ASN.1
- Un byte che specifica la lunghezza della struttura seguente
- Un byte 0x02 per indicare un intero.

- **r**: La lunghezza del valore r seguita dal valore r stesso, codificato come un intero big-endian.
- Un altro byte 0x02 per indicare un secondo intero.
- **s**: La lunghezza del valore s seguita dal valore s stesso, anche questo codificato come un intero big-endian.

È importante notare che se il primo byte di r o s è maggiore di 0x7F, deve essere preceduto da un byte 0x00 per garantirne l'interpretazione come numero positivo.

Il formato DER è stato scelto da Satoshi Nakamoto per serializzare le firme nel protocollo Bitcoin, probabilmente perché era già definito nel 2008, supportato dalla libreria OpenSSL usata all'epoca, ed era abbastanza semplice da adottare senza dover creare un nuovo standard.

VOUT

Livello: avanzato

Argomento: tecnologia

Un VOUT è un numero di indice per un output di transazione.

Una transazione può avere più output, quindi a ciascuno viene assegnato un numero in modo che possa essere referenziato individualmente in seguito.

In programmazione, si inizia a contare da zero. Pertanto, il primo output di una transazione ha un VOUT pari a 0.

A cosa serve il VOUT?
Si utilizza un VOUT in combinazione con un TXID per aiutarti a selezionare un output da spendere come input in una transazione.

Il VOUT svolge un ruolo fondamentale quando si devono creare nuove transazioni. Viene utilizzato in combinazione con il TXID (Transaction ID) per identificare con precisione quale output si intende spendere come input in una nuova transazione. Per comprendere meglio: quando stai costruendo una nuova transazione Bitcoin e devi specificare gli input, devi:

Identificare la transazione precedente che ha creato l'output che vuoi spendere (usando il TXID) Selezionare l'output specifico all'interno di quella transazione (usando il VOUT)

Ogni singolo output nella blockchain può essere referenziato utilizzando la combinazione unica di TXID:VOUT. Questo è chiamato "outpoint".

Il concetto di VOUT è fondamentale quando si parla di transazioni Bitcoin perché permette di identificare con precisione quale output è stato creato in una transazione specifica e che può essere speso successivamente. Ogni transazione sulla blockchain dispone di un set di output, ciascuno con un valore definito e uno script di blocco, noto come scriptPubKey. Quando un utente decide di

spendere Bitcoin, effettua una nuova transazione che prende gli output non spesi (UTXO) delle precedenti transazioni come input. Il VOUT, insieme al TXID della transazione originale, è utilizzato per indicare esattamente quale output si sta cercando di spendere. Questa struttura consente ai nodi della rete di verificare facilmente la validità degli input di una transazione, assicurandosi che l'utente abbia effettivamente il controllo sugli output che intende utilizzare.

2FA

Acronimo di: two-factor authentication

Autenticazione a 2 fattori

Livello: base

Argomento: tecnologia

È un sistema avanzato per la protezione del proprio account, atto ad impedire a terzi di accedere all'account anche nel caso dovessero conoscere username o email e password.

Il 2FA può essere disponibile in diverse modalità: un'app di autenticazione (come Google Authenticator, Microsoft Authenticator, Authy e FreeOTP per citarne alcuni); una chiave di sicurezza fisica (ad esempio Yubikey e Google Titan).

Può essere reso disponibile anche tramite l'invio di un codice su SMS, collegata a un numero di telefono, ma questa modalità si è dimostrata molto vulnerabile per la facilità con le quali è possibile effettuare un attacco SIM-swap, ovvero sostituzione della SIM telefonica.

5$ wrench attack

Attacco con una chiave inglese da 5 dollari

Livello: intermedio

Argomento: legale

Si riferisce al fatto che se qualcuno sa che possiedi criptovalute, può attaccarti fisicamente o minacciarti per farti rivelare la chiave.

Il termine proviene da una vignetta del sito XKCD, nella quale l'idea che la chiave delle criptovalute sia troppo complessa per essere "craccata", in realtà viene raggirata da un attaccante che dice all'altro "il suo laptop è crittato, drogalo e colpiscilo con questa chiave inglese da 5 dollari finché non ci dice la password".

51% Attack

Attacco con il 51%

Livello: base

Argomento: tecnologia

Con attacco al 51%, nel contesto delle blockchain e in particolare di Bitcoin, si intende il caso nel quale un'entità o un gruppo di entità controlla più del 50% della potenza di calcolo totale della rete in una blockchain basata su Proof of Work, come Bitcoin.

Questo livello di controllo consente agli attaccanti di compromettere l'integrità del sistema alterando il normale funzionamento del protocollo di consenso.

Implicazioni e rischi Se un attore malevolo raggiunge la maggioranza dell'hash rate, può:

- **Manipolare la blockchain** scegliendo quali transazioni includere nei blocchi, potenzialmente censurando transazioni specifiche.
- **Impedire la conferma di nuovi blocchi**, ostacolando l'attività di miner onesti e rallentando l'intera rete.
- **Effettuare il double-spending** (doppia spesa), ovvero rispendere gli stessi bitcoin annullando transazioni precedenti e creando una versione alternativa della blockchain (fork).
- **Superare i miner onesti nella creazione di blocchi**, generando una catena più lunga che i nodi considerano valida, escludendo transazioni legittime.

Limitazioni dell'attacco Un attacco del 51% non permette di:

- Creare nuovi bitcoin dal nulla.
- Modificare transazioni già consolidate nella blockchain più lunga prima dell'attacco.
- Accedere ai fondi degli utenti senza conoscere le relative chiavi private.

Costi e difficoltà di un attacco al 51% Sebbene un attacco del 51% sia teoricamente possibile, nel caso di Bitcoin è altamente improbabile a causa dell'enorme potenza di calcolo necessaria. I principali ostacoli sono:

- **Costi elevati**: mantenere più del 50% dell'hash rate richiede hardware specializzato (ASIC), infrastrutture e un consumo energetico colossale.
- **Rischi economici per l'attaccante**: minare la fiducia in Bitcoin ridurrebbe il valore della criptovaluta, rendendo l'attacco economicamente svantaggioso.
- **Contromisure della rete**: in risposta a un attacco, gli sviluppatori e la comunità potrebbero adottare misure difensive, come modifiche al protocollo o fork per neutralizzare l'attaccante.

Nel caso di Bitcoin, grazie alla sua elevata decentralizzazione e alla distribuzione globale dei miner, un attacco del 51% è considerato improbabile e insostenibile nel lungo periodo.

Adaptor signatures

Livello: avanzato

Argomento: tecnologia

Una adaptor signature è una firma aggiuntiva che viene combinata con una firma iniziale per rivelare un dato segreto.

Le adaptor signature consentono a due parti di rivelare reciprocamente due dati contemporaneamente, il che risolve il problema di fiducia coinvolto nelle transazioni simultanee come gli atomic swaps e i coin swaps.

L'impostazione per una adaptor signature prevede un valore segreto, una adaptor signature e una firma "normale". Conoscere due di questi dati è sufficiente per calcolare il terzo.

Una caratteristica potente delle adaptor signature è che una parte può generare una adaptor signature basato su un dato segreto e un'altra parte può generare la propria adaptor signature basata sugli stessi dati senza effettivamente conoscere i dati stessi.

Le Adaptor signatures (chiamate anche signature adaptors) sono dati di firma ausiliari che fanno un commit ad un valore nascosto. Quando un adaptor viene combinato con una firma corrispondente, rivela il valore nascosto. In alternativa, se combinato con il valore nascosto, l'adaptor rivela la firma. Altre persone possono creare adaptor secondari che riutilizzano il commitment anche se non conoscono il valore nascosto. Ciò rende gli adaptor un potente strumento per implementare il lock nei contratti bitcoin.

I contratti in Bitcoin richiedono spesso un meccanismo di lock per garantire l'atomicità di una serie di pagamenti: o tutti i pagamenti vanno a buon fine o tutti falliscono. Questo lock è stato tradizionalmente eseguito facendo in modo che tutti i pagamenti nel set si impegnino nella stessa preimage di hash digest; quando la parte che conosce la preimage lo rivela on-chain, tutti gli altri lo apprendono e possono sbloccare i propri pagamenti.

Gli *hashlock* comunemente usati in Bitcoin consumano circa 67 byte e rivelano il collegamento tra l'insieme di pagamenti perché utilizzano tutti la stessa preimage e digest.

In confronto, i signature adaptor non devono mai essere pubblicati on-chain. Per chiunque non abbia un adaptor corrispondente, una firma creata con un adaptor assomiglia a qualsiasi altra firma digitale, offrendo agli adaptor significativi vantaggi in termini di efficienza e privacy rispetto agli hashlock.

Esempio I molteplici usi dei signature adaptor possono essere visti in un semplice protocollo coinswap. Ad esempio, Alice può fornire a Bob un adaptor per una transazione non firmata che promette di pagargli 1 BTC. Un adaptor da solo non può essere utilizzato come firma BIP340 (Schnorr), quindi Alice non ha ancora pagato Bob.

Ciò che l'adaptor fornisce a Bob è un commitment per il valore nascosto di Alice. Questo commitment include un parametro che Bob può utilizzare per creare un secondo adaptor che si impegna allo stesso valore nascosto dell'adaptor di Alice. Bob può prendere quel commitment anche senza conoscere il valore nascosto di Alice o la propria firma per quel commitment. Bob dà ad Alice il suo adaptor e una corrispondente transazione non firmata che promette di pagarle 1 BTC.

Alice ha sempre saputo il valore nascosto, quindi può combinare il valore nascosto con l'adaptor di Bob per ottenere la sua firma per la transazione che la paga. Trasmette la transazione e riceve il pagamento di Bob. Quando Bob vede quella transazione onchain, può combinare la sua firma con l'adaptor che ha dato ad Alice, permettendogli di ricavare il valore nascosto. Quindi può combinare quel valore nascosto con l'adaptor che Alice gli ha dato in precedenza. Bob trasmette quella transazione per ricevere il pagamento di Alice, completando il coinswap.

Oltre ai coinswap, ci sono molti altri usi proposti per le firme degli adaptor.

Relazione con firme multipartitiche I signature adaptor di solito non possono garantire un contratto completamente da soli. Ad esempio, nella descrizione sopra di un coinswap, Alice potrebbe fare un double spend del suo pagamento a Bob dopo aver appreso la firma di Bob, oppure Bob avrebbe potuto provare lo stesso al contrario (con più difficoltà poiché abbiamo presunto che la transazione di Alice avesse una conferma). Questo problema viene in genere risolto combinando i signature adaptor con le firme multiparty. Ad esempio, Alice deposita i suoi soldi in un indirizzo che può essere speso solo se sia lei che Bob collaborano per creare una firma valida. Ora Alice può fornire a Bob un adaptor per la sua metà della firma multiparty, che Bob può accettare con perfetta sicurezza sapendo che Alice non potrebbe fare un double spend dei fondi senza la sua partecipazione. Ciò potrebbe inoltre richiedere un'opzione di rimborso con timelock, a tempo determinato, nel caso in cui una delle parti si rifiuti di firmare.

Nello schema di firma schnorr, i signature adaptor vengono solitamente proposti per essere combinati con schemi di firma multiparti come MuSig per consentire alla firma pubblicata di sembrare una firma di una sola parte, migliorando la privacy e l'efficienza. Ciò è possibile anche in ECDSA, ma richiede nuovi algoritmi che sono relativamente lenti o richiedono ulteriori presupposti di sicurezza. Invece, esiste uno schema alternativo per le firme degli adaptor per Bitcoin che utilizza 2-of-2 OP_CHECKSIG multisig; questo è meno efficiente e forse meno privato, ma probabilmente più semplice e sicuro dell'ECDSA multipartitico.

addr v2

Livello: avanzato

Argomento: tecnologia

addr v2 è una nuova versione proposta del messaggio addr nel protocollo di rete Bitcoin P2P, che viene utilizzato per pubblicizzare gli indirizzi dei nodi che accettano connessioni in entrata.

Il messaggio addr originale consente l'inoltro di indirizzi IPv6 a 128 bit con compatibilità con le versioni precedenti per IPv4 e indirizzi con codifica onioncat versione 2 (v2) Tor hidden service (.onion).

Tuttavia, gli indirizzi dei servizi nascosti v3 Tor hanno una dimensione di 256 bit, così come gli indirizzi per molti altri protocolli di rete per il miglioramento della privacy. Poiché questi tipi di indirizzo più recenti non possono essere utilizzati con il messaggio addr esistente, è stata proposta una nuova versione del messaggio. Inoltre, l'aggiornamento può consentire di modificare altri aspetti del messaggio o il comportamento dei nodi e dei client che lo elaborano.

Address

Indirizzo

Livello: base

Argomento: tecnologia

L'indirizzo Bitcoin identifica il mittente o il destinatario all'interno di una transazione, e viene utilizzato ad esempio per fare riferimento al wallet di un altro utente su cui effettuare un pagamento e identificarlo nella blockchain.

La creazione degli indirizzi avviene partendo dalla generazione di una chiave privata, che può essere rappresentata per comodità attraverso una frase mnemonica: da tale chiave privata viene generata la corrispondente chiave pubblica e da questa l'indirizzo pubblico.

Nelle prime transazioni, chiamate P2PK, veniva utilizzata direttamente la chiave pubblica in chiaro.

Gli indirizzi bitcoin possono avere diversi formati:

- **1** Gli indirizzi legacy, ovvero quelli nel formato iniziale (P2PKH) hanno il prefisso 1, ad esempio: 12higDjoCCNXSA95xZMWUdPvXNmkAduhWv
- **3** gli indirizzi che iniziano con 3 possono essere di diverso formato:
  - P2SH, usato ad esempio per multisig 3CK4fEwbMP7heJarmU4eqA3sMbVJyEnU3V
  - Nested SegWit P2SH-P2WPKH
  - Wrapped SegWit
- **5** le chiavi private in formato WIF hanno il prefisso 5

- **bc1** Native Segwit P2WPKH con l'aggiornamento del 2017, chiamato SegWit, si sono introdotti gli indirizzi SegWit noti come indirizzi bc1 perché iniziano con iniziano con i caratteri bc1, utilizzando come codifica il formato bech32, ad esempio bc1q34aq5drpuwy3wgl9lhup9892qp6svr8ldzyy7c
- **bc1p** P2TR con l'aggiornamento Taproot sono stati introdotti gli indirizzi codificati con Bech32m, una versione modificata dello schema di codifica Bech32. Bech32m è quasi identico a Bech32: usa solo lettere minuscole, inizia con bc1 per gli indirizzi SegWit.

Il termine indirizzo o address viene criticato perché rischia di utilizzare un termine conosciuto in modo fuorviante. È stato anche fatta una proposta o BIP, la BIP 179, con lo scopo di proporre un nuovo termine per *indirizzo* con il termine invoice (da tradurre in italiano come "richiesta di pagamento" e non "fattura"), che è il termine predefinito nel protocollo Lightning per i pagamenti ed è in realtà più accurato, dal punto di vista tecnico. È più preciso perché le transazioni in bitcoin non hanno un "indirizzo di provenienza", anche se si potrebbe pensare che ce l'abbiano, soprattutto se ci siamo adagiati alla metafora dell'"indirizzo".

Il concetto di "indirizzo di provenienza" ("from address") esiste solo a livello euristico. Una transazione bitcoin non contiene un indirizzo di provenienza, ma output spendibili o UTXO. Una transazione contiene solo gli script, che sono puzzle crittografici e soluzioni degli stessi. Se si riesce a risolvere il puzzle, si possono spendere o meglio trasferire le monete.

È possibile comprendere Bitcoin conoscendo come funzionano le transazioni, che possono avere più ingressi e più uscite.

Non ci sono coin o monete che si muovono da un indirizzo all'altro in bitcoin perché ogni transazione "distrugge" tutti gli input e crea nuovi output. Se si vuole pensare all'analogia con le monete - cioè se si considera ogni UTXO come una moneta di dimensioni diverse - si può pensare a ogni transazione come a un processo di fusione. Tutti gli input vengono liquefatti in una grande fornace e come output vengono create nuove monete.

Il primo indirizzo Bitcoin potrebbe essere considerato il 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa verso il quale è stato trasferito il premio di 50 Bitcoin del genesis block.

Address reuse

Riutilizzo dell'indirizzo

Livello: avanzato

Argomento: tecnologia

Quando viene effettuato un pagamento Bitcoin, in genere deve essere specificato l'indirizzo di destinazione. Quindi l'utente che vuole ricevere l'importo comunica l'indirizzo dove riceverlo.

I wallet degli utenti sono in grado di generare diversi indirizzi, tutti gestiti dallo stesso wallet.

È quindi semplice, ed è consigliato, per ogni pagamento che si deve ricevere anche dallo stesso pagante, utilizzare un nuovo indirizzo di ricezione, evitando il *Riutilizzo degli indrizzi* o **Address Reuse**, che è una pessima pratica ché compromette la privacy e la sicurezza.

Il riutilizzo dell'indirizzo danneggia la privacy non solo di voi stessi, ma anche di altre persone, comprese quelle non collegate alla transazione.

Considerato che un wallet HD (e la maggior parte dei wallet lo sono) può creare un numero di chiavi praticamente infinite, è meglio usare un nuovo indirizzo per ogni nuovo pagamento che si vuole ricevere.

Quando gli indirizzi vengono riutilizzati, permettono ad altri di determinare in modo molto più semplice e affidabile che l'indirizzo riutilizzato è il vostro. Ogni volta che la chiave privata dell'indirizzo riutilizzato firma una nuova transazione, chiunque la riceva può utilizzare le cronologie di quell'indirizzo per scoprire informazioni su di voi, e chiunque sia interessato a scoprire l'identità del proprietario dell'indirizzo ha un obiettivo in più che può cercare di contattare per scoprire chi siete.

Il grafo delle relazioni di un indirizzo riutilizzato è fortemente collegato, in quanto tutti gli input di quell'indirizzo sono necessariamente collegati a tutti i suoi output.

Sono state condotte ricerche significative sull'area di quello che i ricercatori chiamano "collasso dell'identità", ovvero ciò che accade quando più di un indirizzo Bitcoin è fortemente collegato a un altro attraverso il grafo delle transazioni Bitcoin. Il riutilizzo degli indirizzi rende il loro lavoro banale. Esistono database noti al pubblico che non solo hanno fatto collassare milioni di indirizzi Bitcoin, ma hanno anche utilizzato informazioni pubblicamente disponibili per collegare le identità collassate alle persone, e questi database vengono mantenuti attivamente.

Mentre a voi può andare bene che un ricercatore europeo a caso sia obbligato dal suo comitato etico a nascondere la vostra identità al grande pubblico, è molto probabile che le persone che accettano denaro da voi non siano a conoscenza della vostra decisione: quindi, attraverso la vostra azione di riduzione della privacy, le persone che si trovano più avanti nella catena di firma degli indirizzi potrebbero mettervi a rischio se spendono i loro bitcoin in qualcosa che attira l'attenzione delle forze dell'ordine.

Non sempre questo riutilizzo di indirizzi viene fatto dal legittimo proprietario, ma può essere anche causato da un dust attack, dove un attaccante invia piccole quantità di bitcoin a indirizzi che sono già apparsi sulla blockchain, producendo un riutilizzo degli indirizzi anche per gli utenti che consapevolmente hanno cercato di evitarlo.

Alcuni wallet cercano di risolvere questo problema implementando la coin selection, o coin control, obbligatoria che aiuta a evitare che gli utenti spendano dust nelle transazioni nelle quali vogliono proteggere la loro privacy. Altri wallet offrono funzioni opzionali che consentono di spendere tutte i coin ricevuti allo stesso indirizzo contemporaneamente, ma non più di una volta, eliminando la perdita di privacy derivante dal riutilizzo degli indirizzi con il rischio di non poter spendere i fondi ricevuti a un indirizzo precedentemente utilizzato.

L'Address Reuse viene chiamato anche Output linking, in riferimento al fatto che gli importi sono su output, o UTXO, diversi, ma attraverso l'uso di uno stesso indirizzo si riesce a collegarli.

Air-gapping

Livello: avanzato

Argomento: tecnologia

Air gap o dispositivi air gapped, in italiano traducibile in "isolamento fisico", è un metodo per proteggere i computer in cui il dispositivo non si connette a Internet o ad altre reti aperte.

Il concetto di air gap si riferisce a quanto segue: se non è possibile accedere ai dati, non possono essere infettati o danneggiati. Nel settore IT, questo viene in genere implementato come una copia duplicata dei dati di produzione su un sistema di archiviazione secondario, che è offline e come tale non è connesso a nessuna rete di produzione o pubblica.

Nel settore Bitcoin e cripto, con funzionamento funzionamento airgap si intende un device che ospita le chiavi private, ad esempio un hardware wallet, senza che questo sia collegato a Internet, e neanche a un computer o a un cellulare.

L'airgap è quindi una misura di sicurezza che isola fisicamente un dispositivo da una rete non attendibile, come Internet, rimuovendo tutte le interfacce di rete.
I computer airgap sono utilizzati, ad esempio, nelle infrastrutture critiche per la sicurezza. Si tratta di un principio efficace in generale, ma di solito i dati devono essere scambiati con i dispositivi connessi alla rete per normali operazioni.
Questi dati, che devono passare attraverso il sistema di isolamento del device, vengono comunemente trasferiti utilizzando unità flash USB.
La sicurezza di un sistema air-gapped si basa completamente sul fatto che i dati scambiati non vengano alterati in modo dannoso o maligno durante il trasferimento.

È comunque stato dimostrato che la mancata ispezione dei dati scambiati può vanificare i vantaggi della sicurezza, sia per sistemi informatici che per i wallet hardware di criptovalute.

Per quanto riguarda i wallet di criptovalute, il termine airgap indica che un dispositivo di firma come un wallet hardware (che protegge le chiavi private di firma) e un computer in rete potenzialmente insicuro (che viene utilizzato per

creare transazioni non firmate e poi trasmettere le transazioni firmate) sono fisicamente isolati e non direttamente collegati tra loro.
Qualsiasi comunicazione tra i due dispositivi deve colmare il "vuoto", di solito scambiando fisicamente una scheda SD o scansionando codici QR.
È importante notare che la comunicazione esiste e deve esistere. Tale comunicazione include le transazioni di cui sopra, ma anche quantità relativamente grandi di dati per l'aggiornamento del firmware in esecuzione sul wallet hardware o informazioni sul wallet stesso (ad esempio le chiavi pubbliche, alias indirizzi, per la ricezione delle monete).

Invece di collegare un wallet hardware a un computer, un wallet hardware air-gapped utilizza un'applicazione software *companion* installata sul computer che supporta le PSBT (Partially Signed Bitcoin Transactions). Nell'applicazione si crea una transazione non firmata, che viene codificata in un codice QR che può essere scansionato con il wallet hardware, oppure la transazione viene memorizzata come file che viene poi letto dal wallet hardware, di solito da una scheda microSD.
Dopo aver firmato la transazione con le chiavi private, il wallet hardware restituisce la transazione firmata al computer visualizzandola come codice QR sul suo display o scrivendo un altro file sulla scheda microSD. L'applicazione *companion* sul computer importa la transazione firmata e può quindi trasmetterla alla rete.
L'assenza di un collegamento fisico tra i due dispositivi rende più facile percepire la connessione come "sicura". Allo stesso tempo, collegare un portafoglio hardware al computer nello stesso modo in cui si collega una chiavetta USB potrebbe non sembrare altrettanto sicuro.
I vantaggi percepiti e pubblicizzati in termini di sicurezza, potrebbero però essere sovrastimati e portare a un falso senso di sicurezza.

Airdrop

Livello: intermedio

Argomento: finanza

È una operazione generalmente con finalità di marketing che consiste nell'invio di coin o token verso wallet di utenti al fine di promuovere la consapevolezza di una nuova valuta virtuale, spesso in modo gratuito o condizionata a qualche tipo di attività, come la promozione della cripto su un social network.

Altri motivi per l'airdrop possono essere un allineamento di interessi, un segno di apprezzamento, meccanismi di ottenimento alternativi e un'equa distribuzione dei token.

In altre parole, le criptovalute possono essere trasferite per aumentare la consapevolezza, aggirare restrizioni legali o semplicemente per sincera gratitudine.

In generale, per ricevere un airdrop di criptovalute, gli utenti devono soddisfare determinati requisiti, come ad esempio possedere una determinata quantità di criptovaluta o avere un account su una specifica piattaforma di criptovaluta.

Una volta che gli utenti hanno soddisfatto i requisiti, ricevono gratuitamente la criptovaluta in questione direttamente nel loro wallet digitale.

Un airdrop è un'operazione, solitamente con finalità di marketing, che consiste nella distribuzione gratuita di criptovalute (coin o token) direttamente nei wallet degli utenti.
L'obiettivo principale è promuovere la consapevolezza e l'adozione di una nuova valuta digitale o di un progetto blockchain, incentivando l'interesse e la partecipazione della comunità.

Tipologie di Airdrop Gli airdrop possono essere suddivisi in diverse categorie, tra cui:

- Airdrop promozionali: i token vengono distribuiti gratuitamente a chi compie specifiche azioni, come seguire un progetto sui social media, iscriversi a una newsletter o invitare altri utenti.
- Airdrop per holder (o di fidelizzazione): vengono assegnati token agli utenti che possiedono una determinata criptovaluta in un dato momento (snapshot).
- Airdrop di governance: distribuiti per incentivare la partecipazione degli utenti nella governance di una blockchain o di una DAO (Organizzazione Autonoma Decentralizzata).
- Airdrop di fork: avvengono quando una blockchain viene divisa (hard fork) e gli utenti della catena originale ricevono token della nuova blockchain.

Motivazioni e vantaggi

Oltre alle finalità di marketing, un airdrop può essere utilizzato per:

- Incentivare l'adozione: distribuendo token gratuiti, si facilita l'ingresso di nuovi utenti nel progetto.
- Allineare gli interessi degli utenti: chi riceve i token può essere incentivato a utilizzare la piattaforma o il servizio associato.
- Decentralizzare la distribuzione dei token: evitando la concentrazione nelle mani di pochi investitori.
- Riconoscere e premiare la community: come segno di gratitudine per il supporto al progetto.

Rischi e considerazioni Non tutti gli airdrop sono legittimi, alcuni possono nascondere truffe o tentativi di phishin.

È consigliabile:

- Evitare di fornire chiavi private o credenziali per ricevere un airdrop.
- Verificare la fonte e la reputazione del progetto prima di partecipare.
- Prestare attenzione a token sconosciuti che appaiono nei wallet, poiché potrebbero essere collegati a schemi fraudolenti (es. dusting attack).

Gli airdrop nascono come strumento per spingere progetti emergenti, ma è sempre necessaria cautela per evitare rischi legati alla sicurezza, alla privacy, e al rischio che l'incremento di valutazione di un token a seguito della crescita tramite gli airdrop della comunità che lo adotta possa comunque avere un repentino crollo della sua valutazione.

Altcoin

Livello: base

Argomento: tecnologia

Con Altcoin, abbreviazione di 'alternative coin', si intende qualsiasi criptovaluta diversa da Bitcoin.

Ci sono decine di migliaia di criptovalute scambiate in tutto il mondo, tra cui Litecoin LCT, Ethereum ETH, Dogecoin e tantissime altre.

Nella categoria Altcoin possono essere considerati anche token che non sono vere e proprie coin, che non hanno una loro blockchain ma che usano quella di un'altra crypro.

Le altcoin sono create da sviluppatori che vorrebbero migliorare o modificare Bitcoin in qualche modo, proponendo delle varizioni a Bitcoin. Molte di queste presunte migliorie spesso sono pretestuose.

Il proliferare di altcoin non è una cosa buona per diversi motivi, il proliferare di altcoin nasce per o può portare a frodi e truffe.

Alcune altcoin sono create da truffatori che sfruttano la relativa semplicità per essere implementate e cercano di trarre profitto dai consumatori.
È importante fare le proprie ricerche prima di investire in qualsiasi altcoin.

Ci sono troppe altcoin, ed è molto improbabile per una qualsiasi di esse raggiungere una massa critica e diventare un'opzione di pagamento accettata a livello globale.

Spesso non hanno neanche una proposta tecnologica o un reale scopo se non quello speculativo capitalizzando sulla popolarità di Bitcoin, e per questo motivo le altcoin vengono definite shitcoin; tra queste in particolare ci sono le Meme coin.

Altcoin season

Livello: intermedio

Argomento: finanza

La altcoin season, letteralmente Stagione delle altcoin, è un periodo di tempo durante il quale le criptovalute alternative al Bitcoin, chiamate anche altcoin,

tendono ad aumentare di valore rispetto appunto a Bitcoin che è la prima, più diffusa e conosciuta cryptovaluta.

La altcoin season si verifica quando gli investitori iniziano a spostare i loro investimenti verso altre criptovalute invece che verso il Bitcoin, spesso a causa della percezione che queste ultime possano offrire maggiori opportunità di guadagno.

Durante la altcoin season, è comune che le altcoin registrino un aumento significativo del valore, mentre il valore del Bitcoin tende a rimanere stabile o anche a diminuire. È comunque importante evidenziare che il mercato delle criptovalute è altamente volatile, il che le rende più appetibili agli investitori più scalti ma che può rappresentare una trappola per quelli meno esperti poiché i prezzi cambiando rapidamente e in modo imprevedibile potrebbero comportare perdite irrimediabili.

Pertanto, gli investitori dovrebbero fare molta attenzione quando decidono di investire in altcoin e assicurarsi di comprendere i rischi associati a questo tipo di investimento. La crescita del valore di una altcoin potrebbe essere creato ad arte tramite operazioni di Pump & Dump e essere anche sintomo di un possibile Rug Pull.

Durante le altcoin season, vengono riproposte argomentazioni quali dominio di Bitcoin, il rapporto tra il valore di mercato di Bitcoin e il valore di mercato combinato delle altre cryptovalute, o il Flippening.

AMA

Acronimo di: Ask me anything

Livello: base

Argomento: politica

Questa abbreviazione è nata sul forum Reddit, significa "chiedimi qualsiasi cosa", e si riferisce ad un formato di discussione online, in cui una persona, spesso un esperto o una celebrità, risponde alle domande poste da un pubblico di partecipanti.

L'obiettivo di un AMA è quello di permettere alla persona che risponde di condividere la propria conoscenza e le proprie esperienze con gli altri e di offrire agli utenti l'opportunità di fare domande su qualsiasi argomento.

Il fatto che vengano fatte le domande, non significa però che il soggetto risponderà; nel caso di reddit ad esempio, le domande vengono votate da altri utenti, che possono votarle positivamente o negativamente, in modo da incitare il soggetto a rispondere alle domande che con maggiori voti positivi.

Gli AMA sono spesso ospitati su forum o subreddit dedicati, dove gli utenti possono postare le loro domande e ricevere risposte in tempo reale.

AML

Acronimo di: Anti Money Laundering

Anti riciclaggio

Livello: base

Argomento: legale

Le norme anti-riciclaggio (AML, sigla inglese per "Anti-Money Laundering") sono state create con l'obiettivo di prevenire e contrastare il riciclaggio di denaro illecito, ovvero il processo attraverso il quale il denaro guadagnato illegalmente viene "pulito" e reintrodotto nell'economia legale.

Le norme AML sono state istituite in molti paesi per proteggere il sistema finanziario dall'uso illecito e per aiutare a prevenire il finanziamento del terrorismo.

Sono una serie di leggi internazionali alla quale vengono sottoposti gli istituti finanziari, e sempre più spesso anche gli exchange di criptovalute, emanate per contrastare le organizzazioni criminali, che richiedono agli istituti finanziari di effettuare KYC, monitorare le transazioni dei clienti, valutarle e segnalare attività finanziarie sospette.

Sempre più spesso viene richiesto agli Exchange centralizzati di essere inquadrati come istituti finanziari ed effettuare queste attività, che influiscono sui principi di anonimità delle criptovalute.

Tuttavia, alcuni critici sostengono che le norme AML possono essere sproporzionate e inefficaci per gli obiettivi che si propongono. In particolare, tali norme sono un pesante aggravio per gli utenti legittimi mentre possono essere evitate da coloro che cercano di riciclare denaro illecito.

Tali pratiche sono fortemente criticate dalla comunità delle cripto; c'è un enorme divario tra l'intento politico e il risultato e ci sono degli studi che dimostrano che gli interventi AML hanno un impatto inferiore allo 0,1 per cento sulle finanze criminali, i costi di conformità superano di oltre cento volte i fondi criminali recuperati e le banche, i contribuenti e i cittadini comuni sono penalizzati più delle imprese criminali che riescono con facilità ad aggirarle.

AMM

Acronimo di: Automated Market Maker

Market Maker Automatizzato

Livello: avanzato

Argomento: finanza

Nelle criptovalute, un AMM è un algoritmo utilizzato, ad esempio su un DEX, che consente di avere uno specifico prezzo o il miglior prezzo per un asset. Nell'economia e finanza tradizionale, un mercato automatizzato è un mercato in cui l'intero processo di negoziazione è gestito da computer. Ciò include la raccolta di ordini, l'esecuzione degli ordini e la gestione delle negoziazioni. Un AMM è un sistema che fornisce liquidità alla borsa in cui opera attraverso il trading automatizzato. I sistemi AMM sono decollati dopo essere stati implementati per la prima volta da Shearson Lehman Brothers e ATD nei primi anni '90 - prima della loro invenzione, gli order book erano creati da esseri umani che iniziavano manualmente le negoziazioni per aumentare la liquidità del mercato. Questo approccio era la ragione di alcuni slippage e latenze nella scoperta dei prezzi sui mercati. Inoltre, i market maker erano anche accusati di manipolazione del mercato. Quando sono stati introdotti, gli AMM hanno risolto tutti i problemi causati dai market maker umani. Ora, questi tipi di sistemi sono stati introdotti anche nelle borse decentralizzate basate su blockchain.

Nelle borse decentralizzate basate su AMM, il tradizionale libro degli ordini è sostituito da Liquidity pool che sono prefinanziati on-chain per entrambi gli asset della coppia di trading. La liquidità è fornita da altri utenti che guadagnano anche un reddito passivo sul loro deposito attraverso commissioni di trading basate sulla percentuale del pool di liquidità che forniscono. Un DEX che ha implementato un AMM è Uniswap. Uniswap è uno scambio decentralizzato basato su Ethereum che permette ai suoi utenti sia di fornire liquidità per guadagnare reddito passivo o scambiare tra vari asset.

AMP

Acronimo di: Atomic Multipath Payment

Pagamento multipercorso atomico

Livello: avanzato

Argomento: tecnologia

Atomic Multipath Payments (AMP) è un'implementazione del concetto di Multipath Payments (MPP) su Lightning Network.

Gli Atomic Multipath Payments (AMP), a volte chiamati Original AMP o OG AMP, permettono a chi spende di pagare hash multipli tutti derivati dalla stessa preimage - una preimage che il ricevente può ricostruire solo se riceve un numero sufficiente di parti.

A differenza del Simplified Multipath Payments (SMP), questo permette al ricevente di accettare un pagamento solo se riceve tutte le singole parti. Ogni parte che usa un hash diverso aggiunge privacy impedendo che i pagamenti separati siano automaticamente correlati tra loro da una terza parte.

L'aspetto negativo è che chi spende seleziona tutte le preimage, quindi la conoscenza della preimage non fornisce la prova crittografica di aver effettivamente pagato il ricevente.

Sia AMP che SMP permettono di suddividere le HTLC di valore più elevato in più HTLC di valore inferiore che hanno più probabilità di successo individuale, quindi uno spender con sufficiente liquidità può utilizzare quasi tutti i suoi fondi in una volta sola, non importa su quanti canali quei fondi siano suddivisi.

Anarcho-capitalism

Anarco-capitalismo

Livello: base

Argomento: politica

Molti dei primi ad adottare Bitcoin erano propugnatori dell'anarco-capitalismo.

L'anarco capitalismo è una filosofia politica che promuove la libera associazione tra individui e la libera impresa in un contesto sociale e economico senza alcuna forma di governo o autorità centrale.

L'anarco capitalismo è una teoria economica e politica che sostiene la completa abolizione dello Stato e delle sue istituzioni, inclusi i sistemi di regolamentazione, di controllo e di protezione della proprietà, e l'adozione di un sistema economico basato sulla libera impresa e sulla proprietà privata. Secondo gli anarco-capitalisti, il libero mercato, senza il controllo statale, sarebbe in grado di fornire i beni e i servizi che le persone desiderano in modo più efficiente e equo.

In altre parole, l'anarco capitalismo è un sistema economico e sociale basato sul principio della libera iniziativa, in cui le persone sono libere di commerciare e di associarsi come meglio credono, senza alcun tipo di interferenza da parte di un governo o di altre autorità. Indica una filosofia politica e una scuola di pensiero che crede nell'eliminazione degli stati centralizzati a favore della proprietà personale, della proprietà privata e dei liberi mercati.

Gli anarco-capitalisti sostengono che il libero mercato è la forma più efficiente e giusta di organizzare la società, poiché permette a ciascun individuo di fare le proprie scelte e di assumersi le proprie responsabilità. Inoltre, sostengono che lo Stato, come entità che esercita il monopolio della violenza legittima, è intrinsecamente oppressivo e che la sua eliminazione contribuirebbe a una maggiore libertà e a una maggiore giustizia sociale.

I detrattori dell'anarco capitalismo sostengono che potrebbe portare a una maggiore disuguaglianza economica e a una minore protezione dei diritti dei lavoratori e dei consumatori, poiché la mancanza di regolamentazione statale potrebbe favorire la concentrazione del potere e delle risorse nelle mani di un numero

ristretto di individui o di aziende. Inoltre, alcuni sostengono che il libero mercato potrebbe non essere in grado di fornire adeguatamente beni e servizi di base, come la salute, l'educazione e la sicurezza, che sono considerati essenziali per il benessere di una società.

Anchor channel

Livello: avanzato

Argomento: tecnologia

Gli Anchor channel sono una caratteristica opzionale per i nodi Lightning.

Quando si attiva un Anchor channel unilaterale, è possibile aumentare le fee di questa transazione di chiusura in base alle esigenze del mercato, unendo un UTXO extra.

Quando si abilitano Anchor channel in LND, è necessario mantenere almeno 10k satoshi per canale con un massimo di 100k satoshis nel wallet on-chain.

Anchor output-based channel, eliminano il fastidio di dover ipotizzare quali potrebero essere le fee on-chain, in quanto consentono a un nodo di aumentare dinamicamente le fee di una commitment transaction in attesa utilizzando CPFP Child Pays for Parent. Gli Anchor channel, disponibili per gli utenti avanzati a partire da lnd v0.10, sono un tipo di canale più sicuro e affidabile, in quanto consentono di effettuare il bumping della commitment transaction nel caso in cui un canale venga chiuso forzatamente (ad esempio perché l'altra parte non risponde).

Ogni volta che il saldo viene aggiornato all'interno di un payment channel, entrambe le parti firmano una nuova commitment transaction. Questa transazione viene trasmessa solo se una parte decide di chiudere il canale unilateralmente. Tuttavia, nei casi in cui un canale può essere stato aperto per un lungo periodo di tempo, la stima iniziale delle commissioni può comportare un pagamento insufficiente o eccessivo delle transaction fee.

L'introduzione degli anchor channel non solo aumenta l'affidabilità e consente di risparmiare sulle fee, ma contribuisce anche ad aumentare la capacità dei canali, riducendo la riserva di commitment fee. Si noti che per poter usufruire di questo nuovo tipo di canale di Lighting channel, sarà necessario aprire nuovi canali.

Anchor outputs

Livello: avanzato

Argomento: tecnologia

Gli Anchor output sono output speciali nelle commitment transaction di Lightning Network, concepite per consentire il fee bumping della transazione. Un

nome precedente della proposta era simplified commitment.

Ogni volta che il saldo cambia in un canale Lightning Network, viene creata una *commitment transaction* e firmata dalle parti partecipanti. La transazione viene trasmessa solo se una parte decide di chiudere unilateralmente il canale (ad esempio perché l'altra parte non risponde). Poiché la trasmissione della commitment transaction può avvenire molto tempo dopo la sua creazione, la commitment transaction può pagare un importo troppo alto o troppo basso in fee di transazione. Pagare un feerate troppo basso può impedire alla commitment transaction di confermare prima della scadenza dei timelock in essa contenuti, consentendo il furto di fondi.

La soluzione è che la commitment transaction paghi un importo minimo di fee e poi permetta a uno dei due partecipanti al canale di applicare un fee bump alla transazione. I primi progetti per ottenere questo risultato utilizzavano il fee bumping RBF Replace-by-Fee, che si scontrava con i problemi di pinning delle transazioni. I progetti successivi hanno utilizzato il fee bumping CPFP Child Pays For Parent e sono arrivati a dipendere dal CPFP carve-out per aggirare il problema del pinning.

Al momento, le versioni più recenti del progetto aggiungono due output alla commitment transaction, una per ogni parte Lightning Network, e richiedono che tutte le altre output nella commitment transaction siano gravate da una condizione OP_CHECKSEQUENCEVERIFY CSV che impedisce loro di essere spese per almeno un blocco.

Per essere pienamente efficace, il protocollo dipende anche dall'implementazione da parte dei nodi Bitcoin full del package relay, in modo che ci sia un modo per far pagare CPFP le commitment transaction anche se i loro feerate sono al di sotto del minRelayTxFee, la quota minima di relay di un nodo. Tuttavia, fino a quando il package relay non sarà disponibile, i nodi Lightning Network potranno limitarsi a pagare un feerate leggermente più alto sulle loro commitment transaction per assicurarsi che vengano accettate dai nodi.

Anti-Exfil

Livello: avanzato

Argomento: tecnologia

Un protocollo Anti-Exfil è una misura di sicurezza progettata per proteggere le chiavi private utilizzate nei protocolli di firma digitale, come quelle basate su schemi di firma Schnorr o ECDSA (Elliptic Curve Digital Signature Algorithm). L'obiettivo principale di un protocollo Anti-Exfil è impedire a un attaccante che ha accesso limitato a un dispositivo contenente la chiave privata di estrarre o esfiltrare informazioni sufficienti per compromettere la chiave stessa.

Come funziona un protocollo Anti-Exfil? Il protocollo Anti-Exfil introduce meccanismi che assicurano che la chiave privata non possa essere utilizzata in modo

non autorizzato o non possa essere esfiltrata, anche se un attaccante riesce a ottenere l'accesso al dispositivo.

Un attacco quale Dark Skippy può essere sventato con un protocollo di tipo anti-exfil (usato appunto da bitbox02 e jade) limitando la capacità dell'HW (hardware wallet) di scegliere in autonomia il nonce. Per farlo, l'app SW (software del wallet) che viene eseguita sul device dell'utente (pc, cell) interagisce con l'HW e chiede all'HW di scegliere un suo nonce, ma impone che venga aggiunto un nonce scelto dal SW. L'hw ha il compito di firmare con le chiavi private che non sono note al SW, mentre il SW che ha il compito di fare il broadcast della transazione, potrà verificare che il suo contributo al nonce sia stato effettivamente utilizzato e sia presente nella chiave pubblica nonce finale. In questo modo l'attacco potrà essere portato a termine solo se sia HW che SW sono compromessi. È necessario che l'HW non conosca il nonce del SW prima di rivelare il suo nonce originale, altrimenti ha di nuovo piena libertà nella scelta del nonce finale. Questo deve essere garantito dal SW. E l'HW non deve utilizzare lo stesso nonce per due diversi nonce host, altrimenti la chiave privata viene divulgata all'host. Ciò si ottiene inviando in anticipo un hash commitment del nonce del SW.

Controllo delle firme: Quando un dispositivo genera una firma digitale, il protocollo Anti-Exfil garantisce che la firma sia generata in modo sicuro e che non possa rivelare informazioni che potrebbero essere utilizzate per dedurre la chiave privata. Ad esempio, l'attaccante non può indurre il dispositivo a generare firme multiple con lo stesso nonce (numero casuale utilizzato una sola volta), una vulnerabilità che potrebbe compromettere la sicurezza della chiave.

Verifica dell'integrità: Prima di consentire la firma di un messaggio, il dispositivo potrebbe verificare l'integrità e l'origine del messaggio per assicurarsi che non sia stato manipolato da un attaccante. Questo meccanismo protegge contro attacchi in cui un attaccante tenta di manipolare i dati da firmare per estrarre informazioni sulla chiave privata.

Limitazioni operative: Il protocollo può introdurre limiti sul numero di operazioni crittografiche che possono essere eseguite con la chiave privata, riducendo le opportunità per un attaccante di ottenere informazioni utili attraverso un attacco iterativo.

Tecniche di blinding: In alcuni casi, il protocollo può utilizzare tecniche di blinding (oscuramento) dei dati da firmare, in modo che l'attaccante non possa correlare le firme ottenute con i dati reali o con la chiave privata.

Applicazioni nel contesto Bitcoin Nell'ambito delle criptovalute come Bitcoin, dove la sicurezza delle chiavi private è cruciale, un protocollo Anti-Exfil può essere utilizzato per proteggere i wallet hardware, i server che gestiscono chiavi private e altri dispositivi critici. In questi casi, l'Anti-Exfil è particolarmente importante per proteggere contro attacchi avanzati in cui l'attaccante ha accesso temporaneo o limitato al dispositivo.

In sintesi: Un protocollo Anti-Exfil è un sistema di sicurezza progettato per impedire che le chiavi private vengano esfiltrate o utilizzate in modo non autorizzato, garantendo la protezione delle firme digitali e mantenendo l'integrità delle operazioni crittografiche, specialmente in ambienti ad alto rischio come quelli legati alle criptovalute.

AOPP

Acronimo di: Address Ownership Proof Protocol

Livello: intermedio

Argomento: legale

AOPP è un protocollo che consente, per i prelievi su wallet non custodial, di firmare un messaggio per dimostrare che l'indirizzo del wallet utilizzato per il prelievo sia di proprietà di chi sta effettuando il prelievo.

Nasce con l'intento di semplificare il processo di verifica dell'indirizzo per gli utenti che ritirano bitcoin da Exchange regolamentati, per soddisfare un requisito in alcune giurisdizioni, quali il Travel rule.

Gli sviluppatori di wallet BlueWallet, Sparrow, e Trezor hanno implementato l'AOPP sui loro wallet, dichiarando poi a gennaio 2022 di rimuovere questo supporto a seguito delle polemiche scatenate dagli utenti che hanno visto un pericoloso trend nell'assecondare le smanie di deanonimizzare le transazioni bitcoin da parte dei governi, e si sono espressi per non implementare questo standard quale atto di sovranità e responsabilità in quanto protegge gli utenti da possibili futuri - e forse peggiori - meccanismi di sorveglianza che vengono implementati su richiesta degli organismi di regolamentazione.

Oltre a rappresentare una polizza assicurativa, non implementare l'AOPP su wallet Bitcoin serve anche come base per combattere del tutto le misure di verifica del portafoglio, misure che rappresentano uno strappo alla privacy individuale e la possibile normalizzazione di una maggiore sorveglianza sulle transazioni finanziarie degli individui.

API

Acronimo di: Application Programming Interface

Livello: intermedio

Argomento: tecnologia

Le API (Application Programming Interfaces, o Interfacce di Programmazione delle Applicazioni) sono un insieme di funzionalità e specifiche che indicano in che modo i componenti software possono interagire, permettendo a due sistemi di comunicare tra loro.

In pratica, le API fungono da intermediario tra due sistemi, permettendo a uno di accedere alle funzionalità di un altro. Chi fornisce un servizio può rendere accessibili le funzionalità del servizio stesso ai suoi utenti senza dover concordare con gli utenti le modalità di interfacciamento, ma semplicemente rilasciando le specifiche delle proprie API.

Le API possono essere utilizzate in molti modi diversi, ad esempio per:

- Consentire a un'applicazione di accedere ai dati di un altro sistema o di utilizzare le sue funzionalità
- Consentire ai sistemi di scambiare dati o informazioni in modo standardizzato
- Semplificare l'integrazione di sistemi e servizi diversi

Le API sono spesso utilizzate per consentire ai sistemi di comunicare tra loro in modo efficace e sicuro, senza dover condividere direttamente il codice sorgente o le informazioni sensibili. Inoltre, le API possono essere utilizzate per creare nuove funzionalità o estendere le funzionalità esistenti di un sistema, senza dover modificare il codice sorgente originale.

In generale, le API sono uno strumento importante per l'integrazione e la comunicazione tra i sistemi informatici e possono essere utilizzate in molti modi diversi per semplificare e ottimizzare i processi di lavoro.

Un esempio di API per Bitcoin potrebbe essere un'API che permette a un'applicazione di accedere alle informazioni sui prezzi di Bitcoin in tempo reale, ottenute da un Exchange. L'API potrebbe fornire funzionalità come:

- Recupero dei prezzi di Bitcoin in tempo reale
- Recupero della storia dei prezzi di Bitcoin
- Recupero dei tassi di cambio tra Bitcoin e altre valute

Un'altra possibile funzionalità dell'API potrebbe essere quella di consentire all'applicazione di inviare e ricevere pagamenti in Bitcoin, utilizzando un indirizzo di portafoglio (un identificativo univoco associato al proprio portafoglio Bitcoin). L'API potrebbe fornire funzionalità come:

- Generazione di nuovi indirizzi di portafoglio
- Invio e ricezione di pagamenti in Bitcoin
- Verifica dello stato di un pagamento

Queste sono solo alcune delle possibili funzionalità che potrebbero essere offerte da un'API per Bitcoin. In generale, le API per Bitcoin possono essere utilizzate per integrare funzionalità da parte di fornitori di servizi Bitcoin in altre applicazioni o sistemi, consentendo di accedere ai dati e alle funzionalità di Bitcoin in modo semplice e standardizzato.

Gli utenti potrebbero utilizzare queste API attraverso dei programmi, quali ad esempio dei bot, che effettuano delle transazioni senza che l'exchange debba valutare i bot stessi, esponendo i relativi servizi tramite API.

Aping in

Livello: intermedio

Argomento: finanza

Aping In o Aping Into, che letteralmente potrebbe essere tradotto come scimmiottare, si riferisce all'acquistare in un progetto senza fare le necessarie verifiche e ricerche sulla validità del progetto stesso, seguendo la folla e hanno acquistato una moneta senza aver fatto le dovute ricerche sul progetto.

Può capitare di sentire appassionati di criptovalute confessare di aver "aped into" un progetto e di aver perso denaro.

Alcuni progetti si basano solo sul fatto che i nuovi trader "aping in", si accodano (o saltano sul carrozzone) sulla base dell'hype che gli sviluppatori hanno costruito attraverso promozioni a pagamento sui vari social. Il più delle volte, questi progetti inconsistenti e privi di un vero e proprio caso d'uso si schiantano non appena gli sviluppatori esauriscono il loro budget pubblicitario e il clamore si esaurisce.

L'Aping-in è spinto fortemente dalla FOMO, dalla lettura di messaggi sui social network che sostengono fortemente il progetto *ma non sono consigli finanziari*

APR

Acronimo di: Annual Percentage Rate

Indice sintetico di costo

Livello: intermedio

Argomento: finanza

APR sta per Annual Percentage Rate, letteralmente Tasso percentuale annuo, indica l'interesse annuo generato da una somma addebitata a chi chiede un prestito o pagata agli investitori.

L'APR viene espresso come percentuale che rappresenta il costo annuo effettivo dei fondi per la durata di un prestito o il reddito guadagnato su un investimento. Ciò include eventuali commissioni o costi aggiuntivi associati alla transazione, ma non tiene conto della capitalizzazione. L'APR fornisce ai consumatori un numero di profitti che possono confrontare tra istituti di credito, carte di credito o prodotti di investimento.

Nelle criptovalute, l'APR è la percentuale che gli investitori possono aspettarsi di guadagnare come interesse sul loro investimento, per prestare la loro cripto o renderla disponibile per i prestiti. L'APR tiene conto di altre commissioni che il mutuatario deve pagare, ma non include l'interesse composto.

In sostanza, l'APR è il tasso di interesse ordinario applicato all'importo principale di un investimento o di un prestito. Poiché l'APR è un tasso annualizzato,

se l'investimento o il prestito sono detenuti per un periodo più breve, viene applicato un interesse proporzionale. Ad esempio, un investimento di sei mesi con un TAEG del 5% frutterà solo il 2,5% del capitale.

L'APR è molto semplice. Prendiamo ad esempio un investimento di 1,0 Ether (ETH) in un pool di prestiti su una rete di finanza decentralizzata (DeFi). Se l'APR espresso è del 24%, si dovrebbero guadagnare 0,24 Ether in aggiunta all'investimento iniziale se questo viene bloccato nel pool per un anno esatto. Di conseguenza, l'investimento dovrebbe ammontare a 1,24 Ether, composto dal capitale di 1,0 Ether e dagli 0,24 Ether di interessi maturati (basato su APR al 24%).

Nel caso della DeFi e in particolare nelle funzionalità di yield farming e nei programmi di incentivazione legati alla fornitura di liquidità, la principale differenza tra APR e APY è che nell'APR l'harvest, ossia la funzione interna allo smart contract del liquidity mining che permette di riscuotere nel proprio wallet le ricompense, viene fatta più di rado e le ricompense non vengono reinvestite portando ad un rendimento minore.

Le istituzioni finanziarie dei mercati regolamentati devono divulgare l'APR di uno strumento finanziario prima della firma di qualsiasi accordo.

APY

Acronimo di: Annualised Percentage Yield

Rendimento percentuale annuo

Livello: intermedio

Argomento: finanza

L'APY, Annualised Percentage Yield o Rendimento Percentuale Annuo, è una rappresentazione normalizzata di un tasso di interesse, basato su un periodo di un anno. I valore dell' APY consente un confronto ragionevole e univoco di diverse offerte con programmi di composizione variabili. Tuttavia, non tiene conto della possibilità che le commissioni sul conto influiscano sul guadagno netto. APY si riferisce generalmente al tasso pagato a un depositante da un istituto finanziario, mentre l'analogo tasso percentuale annuo (APR) si riferisce al tasso pagato a un istituto finanziario da un mutuatario.

Nel caso della DeFi e in particolare nelle funzionalità di yield farming e nei programmi di incentivazione legati alla fornitura di liquidità, la principale differenza tra APR e APY è che nell'APR l'harvest, ossia la funzione interna allo smart contract del liquidity mining che permette di riscuotere nel proprio wallet le ricompense, viene fatta più di rado e le ricompense non vengono reinvestite portando ad un rendimento minore.

Arbitrage

Arbitraggio

Livello: intermedio

Argomento: finanza

L'arbitraggio di criptovalute è una strategia di trading che consiste nell'acquistare una criptovaluta a un prezzo basso su un exchange e vendendola contemporaneamente su un altro exchange che ha prezzo più alto.

Il profitto viene realizzato dalla differenza tra i prezzi di acquisto e di vendita.

L'arbitraggio consente di guadagnare dalle differenze di prezzo esistenti dai vari exchange negli scambi di criptovalute.

L'arbitraggio di criptovalute è complesso e richiede una buona conoscenza del mercato e una attenta analisi dei prezzi, ma può essere un modo per generare profitti in un mercato volatile.

ARTs

Acronimo di: asset-referenced tokens

Livello: avanzato

Argomento: politica

Le definizioni ARTs e EMTs sono stati inseriti nel MiCA, il regolamento sui mercati nei cripto asset proposto dall'Unione Europea.

Gli ARTs sono token ancorati a riserva con valore stabile: monete fiat, commodity, crypto-asset, etc.

Sono definiti come criptovalute che hanno l'obbiettivo di mantenere un valore stabile facendo riferimento al valore di diverse valute aventi corso legale, una o più materie prime o una o più criptovalute, o una combinazione di tali attività.

In altre parole, stablecoin fiat, commodity o criptovalute.

ASIC

Acronimo di: Application Specific Integrated Circuit

Livello: intermedio

Argomento: tecnologia

Un ASIC (Application-Specific Integrated Circuit, circuito integrato per applicazione specifica) è un tipo di circuito integrato progettato su misura per risolvere specifiche applicazioni di calcolo. Questa progettazione su misura consente di ottenere prestazioni notevoli in termini di velocità di elaborazione, ma richiede un consumo elettrico significativo. A differenza dei processori generici

come CPU e GPU, che possono essere utilizzati per una vasta gamma di compiti, l'ASIC si focalizza esclusivamente sulla risoluzione di un unico problema.

Nel contesto della tecnologia block chain, l'ASIC viene spesso menzionato in relazione ai computer di mining. Ad esempio, per il mining di Bitcoin, l'utilizzo di ASIC è considerato indispensabile a causa della quantità effettiva dei calcoli richiesti. I compiti di mining richiedono un'enorme potenza di calcolo e l'efficienza dell'ASIC nella risoluzione di tali calcoli lo rende lo strumento ideale per questa specifica attività.

In sintesi, un ASIC è un circuito integrato specializzato che offre prestazioni elevate per un'attività di calcolo specifica, superando in velocità ed efficienza i processori generici come CPU e GPU.

Nella tecnologia block chain, l'ASIC è particolarmente importante per il mining di criptovalute come Bitcoin, in quanto riesce a gestire in modo efficiente i complessi calcoli necessari per convalidare le transazioni e garantire la sicurezza della rete.

Asicboost

Livello: avanzato

Argomento: tecnologia

Tecnologia di efficientamento degli ASIC Antminer dell'azienda Bitmain (di proprietà di Jihan Wu) che non era compatibile con l'upgrade SegWit.

È stata al centro delle polemiche poiché nel 2017 si accusava Bitmain, Jihan Wu e altri miners sotto la sua influenza di voler boicottare l'aggiornamento a SegWit per non perdere questa ottimizzazione dei suoi Asic per il mining.

Bitcoin Core e Knots 0.18 hanno rimosso il supporto per la creazione di modelli di blocchi non Segwit nel 2019, dopo l'aggiornamento a Taproot l'unico modo per utilizzare ASICBoost è creare un blocco completamente vuoto.

ASN

Acronimo di: Autonomous System Number

Sistema autonomo di rete

Livello: avanzato

Argomento: tecnologia

ASN può essere l'abbreviazione di Autonomous System Network o Autonomous System Number, nel contesto dei protocolli di rete.

Un Autonomous System Network, o sistema autonomo di rete, in riferimento ai protocolli di routing, è un gruppo di router e reti sotto il controllo di una singola e ben definita autorità amministrativa.

Ogni sistema autonomo (AS) è associato a un numero di sistema autonomo (ASN) univoco ed è costituito da un gruppo di prefissi IP che ricadono sotto il controllo di una singola entità amministrativa, come un provider di servizi Internet (ISP).

Nel contesto dei nodi Bitcoin, l'ASN può essere utilizzato per identificare la società o l'organizzazione che gestisce il nodo.

Attraverso dei database di ASN e il geo-tagging degli indirizzi IP, è possibile ipotizzare una probabile collocazione geografica di un nodo.

Tuttavia, è importante tenere presente che non tutti i nodi Bitcoin annunciano i propri percorsi Internet e, di conseguenza, non hanno un ASN associato. Inoltre, un singolo ASN può coprire più nodi Bitcoin. I nodi possono poi essere instradati nella rete TOR, in modo da nascondere l'effettivo indirizzo IP del nodo.

Gli ASN sono fondamentali per determinare i percorsi più efficienti per il traffico di rete utilizzando il Border Gateway Protocol (BGP), che consente a Internet di funzionare come una rete globale e interconnessa.
Una gamma diversificata di ASN è essenziale affinché la rete peer-to-peer di Bitcoin mantenga la sua natura decentralizzata, una caratteristica chiave che la distingue dai sistemi finanziari tradizionali.
Questa diversità migliora anche la resilienza della rete contro potenziali minacce, rendendo più difficile per i malintenzionati interrompere la rete prendendo di mira un singolo punto debole.

Asset

Cespite

Livello: base

Argomento: economia

Un asset, che in italiano può essere tradotto come cespite anche se nel settore delle cripto anche in italiano viene usato il termine inglese asset, è qualsiasi cosa di valore monetario che può essere posseduta o acquistata.

Tradotto a volte con il termine Attività, gli asset e le attività sono concetti finanziari che spesso vengono usati in modo intercambiabile, ma in realtà hanno significati leggermente diversi. Gli asset sono beni materiali o immateriali che possiede un'azienda o un individuo e che hanno un valore economico. Ad esempio, il denaro contante, gli investimenti, le proprietà immobiliari e le attrezzature sono tutti esempi di asset.

Le attività, d'altra parte, sono tutte le risorse economiche che un'azienda o un individuo possiede e che sono utilizzate per produrre beni o servizi. Ad esempio,

il personale, le materie prime e gli equipaggiamenti sono tutti esempi di attività.

In sintesi, gli asset sono beni di proprietà di un'azienda o di un individuo che hanno un valore economico, mentre le attività sono le risorse economiche che un'azienda o un individuo utilizza per produrre beni o servizi.

Nel contesto degli investimenti, gli asset possono riferirsi a una varietà di strumenti finanziari e fisici, dalle azioni agli immobili, dai metalli preziosi, ai dollari.

Bitcoin viene considerato da alcuni come un asset digitale.

Confrontando la capitalizzazione di mercato con gli atri asset, dei quali l'oro occupa la prima posizione, Bitcoin si trova nella classifica dei primi 20, superando a volte Visa.

Un cripto asset o asset crittografico è un tipo di asset digitale, come ad esempio una criptovaluta come Bitcoin, che utilizza la crittografia per garantire la sicurezza e la trasparenza delle transazioni. È un asset digitale che può essere utilizzato come mezzo di scambio o come unità di conto. Può anche essere utilizzato per rappresentare un valore o un'attività nell'economia digitale.

La rappresentazione di un asset può essere effettuata attraverso un token, e in certi casi asset e token vengono utilizzati in modo interscambiabile.

Asset Universe

Livello: avanzato

Argomento: tecnologia

L'Asset Universe, universo degli asset, è una caratteristica di Taro che fornisce informazioni sugli asset, e consente agli utenti e agli emittenti di asset di fornire prove sulla provenienza degli asset, l'emissione di forniture e interagire più facilmente con i dati sugli asset di Taro.

Un Taro universe è un repository di asset e delle loro prove. Un universo può contenere informazioni su uno o più tipi di asset (ad esempio una specifica stablecoin o tutte le stablecoin). Può contenere informazioni su quali asset sono stati emessi, sulla loro quantità e sulle loro regole, oltre a contenere le prove dei trasferimenti recenti. I criteri per il rilascio di queste informazioni sono a discrezione di un universo o di un operatore di universo.

Funziona in modo simile a un block explorer Bitcoin, ma mostra i dati delle transazioni Taro che sono archiviati off-chain con i client Taro.

Un Universo può essere gestito dal solo emittente o dagli stessi emittenti degli asset, o può essere nominato da un emittente quale explorer di un asset. È anche ipotizzabile che gli Universi gestiti dalla comunità aggreghino le informazioni inviate dai possessori delle risorse.

L'operatore di un universo non ha privilegi all'interno del protocollo Taro.

Dato un ID noto di un asset, l'Universo può ad esempio fornire informazioni sul suo Genesis output, oltre alle attuali metainformazioni come la documentazione, gli script degli asset o i token totali in circolazione. Un servizio può anche conoscere più asset (Multiverso) o solo un singolo output (Pocket Universe).

Un Universo non ha privilegi all'interno del protocollo Taro. Produce dati di transazione convalidati rispetto alla blockchain di bitcoin.

Un Universo adversarial potrebbe solo astenersi dal restituire i dati richiesti dai client. I dati delle transazioni Taro non sono vincolati a un Universo. L'offerta di disponibilità dei dati fornita da un Universo è motivata da entità che desiderano avere una verifica veloce ed economica delle loro attività Taro.

Per dare agli utenti/detentori di un asset un modo semplice per ricostruire la provenienza, nonché per tenere traccia della quantità totale di unità emesse per un determinato asset, è necessaria una struttura di indicizzazione merkalizzata on-chain. Inoltre, se definiamo dei vincoli sul modo in cui un Universo "canonico" può essere aggiornato, allora gli utenti sono in grado di guardare un insieme di output on-chain per essere avvisati di ulteriori emissioni della catena. Continuando a basarsi su questa struttura, se gli utenti sono in grado di mantenere un rapporto di fiducia con l'emittente di un asset (ad esempio, l'asset appartiene a un gioco closed source), allora possono delegare i diritti di aggiornamento a un singolo o a un insieme federato di parti, consentendo loro di raggruppare diversi aggiornamenti di asset in un'unica transazione, scalando così i trasferimenti on-chain.

La provenienza degli asset Taro è definita dalla discendenza di un asset fino al punto di genesi, che è l'outpoint da cui deriva l'identificatore univoco dell'asset. Un Universo Taro è proposto come un modo per gli utenti/titolari di un asset di avviare facilmente il riconoscimento di un determinato punto di genesi come radice di un asset.

Un Universo è un MS-SMT merkle-sum Sparse Merkle tree, che indicizza l'insieme degli outpoint spesi che tracciano il movimento/trasferimento di un asset. Un Universo può contenere solo l'insieme degli outpoint di genesi di un asset, più asset, tracciare le singole transazioni ed essere utilizzato anche come livello di aggregazione.

L'MS-SMT di un Taro asset Universe si differenzia dal normale MS-SMT per il fatto che il key index dell'albero più basso è un outpoint piuttosto che un asset script key, poiché dato un outpoint in cui era presente un asset, l'asset Universe mappa alla transazione Taro + i meta dati di spesa. Data questa struttura di indicizzazione degli outpoint, se creiamo un nuovo outpoint "re genesis", possiamo costruire un nuovo grafo virtuale delle transazioni Taro che traccia in modo dimostrabile il movimento degli asset in modo off-chain, affidandosi a una parte singola o federata per gestire gli aggiornamenti.

assume valid

Livello: avanzato

Argomento: tecnologia

Assume Valid è una scorciatoia che consente ai nodi Bitcoin di sincronizzarsi più velocemente con la blockchain.

Assume Valid è un'opzione in Bitcoin Core, abilitata per impostazione predefinita, che assume che tutti gli script fino a una determinata altezza del blocco o Block height siano validi.

Ciò significa che i nuovi full node che sincronizzano la blockchain durante il download iniziale del blocco (IBD) possono saltare la verifica degli script dal Genesis block fino all'altezza del blocco stabilita dal client Bitcoin Core in una determinata versione.

Questi script costituiscono la parte dei dati Witness delle transazioni, principalmente le firme che risolvono gli script di blocco e sbloccano i fondi da spendere, nonché i blocchi temporali e altre condizioni di spesa programmate.

Gli utenti hanno la possibilità di impostare `assumevalid=0` e forzare il loro client a eseguire la verifica completa di tutti gli script, oltre alla verifica degli altri contenuti dei blocchi.
Tuttavia, l'assunzione generale e piuttosto sicura alla base dell'abilitazione predefinita di "Assume Valid" è che sia stata dimostrata una quantità sufficiente di Proof of Work fino a quella determinata altezza del blocco, il che fa ritenere che gli script che la precedono siano validi.

AssumeUTXO

Livello: avanzato

Argomento: tecnologia

AssumeUTXO è una modalità proposta avviare un nuovo full node senza dover attendere il caricamento della intera blockchain, processo chiamato IBD (Initial Block Download) che può durare giorni o settimane prima che il nodo possa partecipare attivamente alla rete Bitcoin.

AssumeUTXO è stato inserito (merged) nel ramo principale di Bitcoin Core a ottobre 2023.

AssumeUTXO consente di posticipare la verifica della vecchia cronologia della blockchain fino a quando l'utente è in grado di ricevere transazioni recenti.

Quando il parametro AssumeUTXO viene utilizzato, i nodi Bitcoin possono saltare il controllo dei dati di input della transazione (ovvero i riferimenti alle transazioni precedenti che hanno prodotto gli output non spesi utilizzati come input) e assumere che gli UTXO richiesti siano già presenti nella blockchain.

Ciò consente di ridurre il tempo di verifica della transazione e di aumentare l'efficienza del processo di validazione dei blocchi.

Assumeutxo consente ai nodi di inizializzarsi utilizzando una versione serializzata dell'UTXO set, l'insieme di tutti i bitcoin spendibili e le condizioni necessarie per spenderli, ad un'altezza del blocco predeterminata.

Analogamente all'impostazione di assumevalid esistente e ad altri parametri utilizzati dai nodi per convergere sul consenso, le revisioni dell'hash di AssumeUTXO verrebbero verificate per correttezza dai programmatori durante la revisione del codice. Ciò consentirebbe agli operatori dei nuovi nodi di fidarsi facoltativamente di tale hash e scaricare un UTXO Set che corrisponde a tale hash. Per i blocchi prodotti successivamente all'hash dell'UTXO Set, il nodo verificherebbe i nuovi blocchi e aggiornerebbe il proprio UTXO Set come qualsiasi altro nodo senza dover fare ulteriori verifiche. Come attualmente progettato, il nodo scaricherebbe e verificherebbe anche i blocchi più vecchi in background in modo da poter eventualmente dimostrare che l'hash con cui ha iniziato era corretto.

ATH

Acronimo di: all time high

massimo storico

Livello: intermedio

Argomento: finanza

ATH, in inglese All Time High tradotto in italiano come massimo storico, è il prezzo più alto che una criptovaluta ha mai raggiunto dalla prima volta in cui è stata quotata su un exchange.

Nel caso dei bitcoin e di altre criptovalute, in genere viene utilizzato come cambio di riferimento il dollaro, ma il termine ATH può riferirsi a diversi cambi delle criptovalute sia con valute fiat che altre cripto.

Ad esempio, il 10 novembre 2021, Bitcoin ha raggiunto un ATH di 69.050 dollari. Questo significa che, in quel momento, Bitcoin era scambiato a un prezzo più alto di quanto non lo fosse mai stato in passato.

Il massimo storico viene misurato da quando l'asset inizia a essere scambiato su un exchange e cambia ogni volta che viene superato il massimo più recente. Il valore di un massimo storico è solitamente nominale, il che significa che l'inflazione non viene considerata. Questo fa in modo che con valute che hanno una forte inflazione potrebbe verificarsi un ATH ma a causa dell'inflazione non si abbiano dei reali guadagni in termini di capacità di acquisto.

I massimi storici in genere rappresentano importanti notizie sui prezzi per i mercati. Gli investitori possono essere motivati ad acquistare azioni ritenendo

che l'asset continueranno a performare bene in futuro. Altri investitori possono essere persuasi a vendere, ritenendo che il prezzo possa in futuro avere una tendenza al ribasso. Gli asset che raggiungono costantemente i massimi storici attirano rapidamente potenziali investitori, mentre quelli che raggiungono ripetutamente i minimi storici dissuadono i potenziali investitori.

ATL

Acronimo di: all Time Low

minimo storico

Livello: intermedio

Argomento: finanza

ATL, abbreviato in All-Time Low, significa "minimo storico". Nel contesto delle criptovalute, l'ATL è il prezzo più basso mai raggiunto da una criptovaluta.

Si contrappone all'ATH, che indica il prezzo più alto mai raggiunto da una criptovaluta.

ATM

Livello: base

Argomento: finanza

Uno sportello automatico (ATM o bancomat) che consente all'utente di acquistare e vendere Bitcoin. Funzionano in modo simile agli ATM o bancomat convenzionali, ma invece di mostrare i dettagli del proprio conto bancario, agli utenti vengono presentate una serie di opzioni per scambiare Bitcoin in cambio di contanti.
I Bitcoin ATM che offrono solo opzioni di acquisto sono indicati come unidirezionali, mentre quelli che offrono funzionalità sia di acquisto che di vendita sono noti come bidirezionali. Non si collegano alla banca di un utente o a una rete bancaria.
Invece, sono essenzialmente interfacce connesse a Internet che consentono all'utente di interagire con un exchange.

A seguito di decreto emesso dal Ministero dell'Economia e delle Finanze, è richiesto ai fornitori di servizi di valuta virtuale (come gestori di ATM di criptovalute) di registrarsi presso l'OAM, Organismo Agenti e Mediatori per monitorare gli scambi di criptovalute e implementare misure AML. Pertanto, dal 1 luglio 2022 gli ATM di criptovalute in Italia richiedono il KYC per tutti gli importi.

Atomic Swap

Livello: avanzato

Argomento: tecnologia

Un modo per consentire alle persone di scambiare tra loro diversi tipi di criptovaluta su diverse blockchain senza dover utilizzare un intermediario centralizzato, quale per esempio l'exchange, attraverso l'uso di appositi smart contract.

Atomicals

Livello: avanzato

Argomento: tecnologia

Atomicals Bitcoin è un protocollo semplice ma flessibile per la creazione, la trasmissione e l'aggiornamento di oggetti digitali (tradizionalmente chiamati token non fungibili) per blockchain UTXO come Bitcoin.

Un Atomical (o "atomo") è un modo per organizzare la creazione, la trasmissione e gli aggiornamenti di asset digitali. È essenzialmente una catena di proprietà digitale definita secondo poche regole semplici.

Ogni Atomical ha un'origine, un proprietario attuale e una serie di regole che governano come può essere trasferito. L'origine di un Atomical può essere un'emissione di nuova moneta, un trasferimento da un altro Atomical o un'operazione di fusione o divisione.

Il proprietario attuale di un Atomical è l'indirizzo Bitcoin che ha la chiave privata che consente di spendere l'output UTXO associato all'Atomical.

Le regole che governano come può essere trasferito un Atomical sono definite nel suo script di trasferimento. Lo script di trasferimento può essere semplice o complesso, a seconda delle esigenze dell'Atomical.

Atomicals Bitcoin offre una serie di vantaggi, tra cui:

- **Sicurezza**: Gli Atomicals sono memorizzati sulla blockchain Bitcoin, che è una rete altamente sicura.
- **Scalabilità**: Gli Atomicals sono relativamente piccoli, il che li rende scalabili per blockchain come Bitcoin.
- **Flessibilità**: Gli Atomicals possono essere utilizzati per creare una varietà di oggetti digitali, tra cui token non fungibili, oggetti di gioco e contratti intelligenti.

Atomicals Bitcoin è ancora in fase di sviluppo.

Ecco alcuni esempi di come Atomicals Bitcoin può essere utilizzato:

- Emissione di token non fungibili: Atomicals Bitcoin può essere utilizzato per emettere token non fungibili (NFT) che rappresentano oggetti digitali unici, come opere d'arte, oggetti di gioco o biglietti per eventi.

- Creazione di oggetti di gioco: Atomicals Bitcoin può essere utilizzato per creare oggetti di gioco che possono essere scambiati e venduti tra i giocatori.
- Implementazione di contratti intelligenti: Atomicals Bitcoin può essere utilizzato per implementare contratti intelligenti che possono essere utilizzati per automatizzare le transazioni e le attività.

Atomicals Bitcoin è un'innovazione promettente che ha il potenziale di aumentare i casi d'uso di Bitcoin.

Attività

Livello: base

Argomento: economia

In ragioneria, in finanza d'impresa ed in economia, Attività ha il significato di Cespite.

In lingua inglese viene a volte tradotto genericamente in Asset, o al contrario Asset viene tradotto in Attività, Asset e Attività sono concetti finanziari che spesso vengono usati in modo intercambiabile, ma in realtà hanno significati leggermente diversi. Gli asset sono beni materiali o immateriali che possiede un'azienda o un individuo e che hanno un valore economico. Ad esempio, il denaro contante, gli investimenti, le proprietà immobiliari e le attrezzature sono tutti esempi di asset.

Le Attività, d'altra parte, sono tutte le risorse economiche che un'azienda o un individuo possiede e che sono utilizzate per produrre beni o servizi. Ad esempio, il personale, le materie prime e gli equipaggiamenti sono tutti esempi di Attività.

In sintesi, gli asset sono beni di proprietà di un'azienda o di un individuo che hanno un valore economico, mentre le Attività sono le risorse economiche che un'azienda o un individuo utilizza per produrre beni o servizi.

La parola Attività viene anche riferita alle Cripto-attività, per le quali si da una definizione specifica.

Auction

Asta

Livello: intermedio

Argomento: finanza

Un'asta è un tipo di mercato che consente ad acquirenti e venditori di interagire tra loro tramite offerte. Le aste hanno i vantaggi di un'elevata liquidità e la possibilità della scoperta dei prezzi.

Austrian school of economics

Economia austriaca

Livello: intermedio

Argomento: economia

L'Economia Austriaca, o Scuola Austriaca di Economia, è una scuola di pensiero economica che prende il nome dalla sua origine in Austria alla fine del XIX secolo. Questa scuola di pensiero si concentra sulla teoria dell'azione umana e sulla libertà individuale come forza motrice dell'economia.

I suoi principali rappresentanti includono Ludwig von Mises e Friedrich Hayek, entrambi vincitori del premio Nobel per l'economia. La loro visione dell'economia si basa sull'idea che le economie sono complesse e dinamiche, e che le informazioni sono diffuse in tutta la società, non solo tra i governi e i grandi imprenditori.

Inoltre, l'economia austriaca rifiuta l'idea che l'intervento del governo nell'economia possa essere efficace o auspicabile. Invece, sostiene che il libero mercato, i prezzi liberi e la proprietà privata sono la base per un'economia prospera.

Alcuni dei concetti chiave dell'economia austriaca includono la teoria del ciclo economico, che spiega come le espansioni monetarie artificiali possono portare a bolle e crisi economiche, e la teoria del valore soggettivo, che sostiene che il valore di un bene è determinato dal suo utilizzo soggettivo per l'individuo che lo possiede.

La Scuola Austriaca di Economia è stata spesso associata al movimento libertario e ad una forte opposizione all'intervento governativo nell'economia. Molti sostenitori della Scuola Austriaca di Economia vedono Bitcoin come una forma di valuta alternativa che consente alle persone di scambiare beni e servizi senza l'intervento dei governi o delle banche centrali.

In particolare, i sostenitori della Scuola Austriaca vedono Bitcoin come un'alternativa al sistema monetario attuale, basato sulle valute fiat e sul controllo da parte delle banche centrali, e sostengono che Bitcoin sia una forma di denaro "hard", cioè una valuta che non può essere manipolata dalle autorità monetarie e che mantiene il suo valore nel tempo.

In sintesi, molti degli ideali della Scuola Austriaca, come la libertà economica e la decentralizzazione, sono anche alla base di Bitcoin.

B-Money

Livello: avanzato

Argomento: economia

A fine anni novanta lo sviluppatore Wei Dai cercò di superare i limiti posti da Paypal tramite l'idea di B-Money, un sistema di pagamento che doveva essere distribuito, digitale ed anonimo.

Questo avveniva attraverso due canali di trasmissione, uno anonimo ed uno pubblico, la cui sincronicità verificava la transazione. Wei Dai non attrasse sufficiente attenzione dagli investitori, ma ebbe l'onore di essere citato da Satoshi Nakamoto.

Bag

Livello: intermedio

Argomento: finanza

Bag, in italiano borsa, è un termine gergale che si riferisce a una particolare detenzione di asset crypto, in genere riferito a una quantità dell'asset superiore alla media.
Sebbene non esista una soglia universale specifica di quanti token o monete esattamente costituiscano una Bag, l'espressione generalmente distingue i diversi tipi di token o monete presenti nel portafoglio di un investitore.

Il concetto di Bag implica un volume significativo di criptovalute, suggerendo una quantità che va oltre la norma o che si discosta dalla media detenuta dagli investitori. Questo termine può essere utilizzato per esprimere l'idea di una detenzione più sostanziosa e diversificata di token o monete digitali, evidenziando la presenza di una varietà di asset nel portafoglio di un investitore.

Inoltre, l'espressione "heavy bag" (borsa pesante) viene talvolta impiegata per descrivere una detenzione particolarmente ampia di una specifica criptovaluta. Questa terminologia sottolinea l'entità significativa della detenzione di un singolo asset digitale all'interno del portafoglio di un investitore, suggerendo un impegno notevole o una particolare fiducia nei confronti di quella specifica criptovaluta.

Bank Run

Corsa agli sportelli

Livello: base

Argomento: finanza

Una corsa agli sportelli bancari, conosciuta come Bank Run, avviene quando i clienti di una banca prelevano denaro perché temono che l'istituzione non abbia abbastanza riserve.

Le banche investono o prestano la maggior parte dei fondi depositati e mantengono solo una quantità limitata di contanti in mano.

Se i clienti richiedono prelievi simultanei e la banca non ha abbastanza denaro contante a disposizione, possono verificarsi difficoltà nel soddisfare le richieste di prelievo. La corsa agli sportelli bancari può portare alla mancanza di liquidità, mettendo a rischio la sopravvivenza della banca. La causa principale delle Bank Run è la diffusione di voci su un'esaurimento delle riserve di denaro della banca o la mancanza di denaro contante in una specifica filiale. Le corse alle banche possono anche verificarsi quando i clienti prelevano denaro tramite trasferimento elettronico. La maggior parte delle banche ha un limite imposto per quanto può essere mantenuto nei depositi ogni giorno.

In caso di corsa agli sportelli bancari, la banca potrebbe non avere abbastanza denaro contante a disposizione per far fronte alla domanda di prelievo. Pertanto, mancano i soldi effettivi necessari per soddisfare le richieste di prelievo. Di conseguenza, le banche si trovano senza denaro man mano che sempre più clienti richiedono prelievi dai loro conti, aumentando la probabilità che collassino o falliscano.

Una delle cause predominanti di una corsa agli sportelli bancari è la rapida diffusione di voci secondo cui una banca sta esaurendo il denaro nella sua riserva depositata. Il sentimento negativo scatena paura e ansia nei clienti che agiscono immediatamente effettuando prelievi senza nemmeno verificare la notizia.

Può anche derivare da una carenza di denaro contante in una specifica riserva. Ad esempio, quando un'agenzia bancaria esaurisce il denaro contante, molti clienti non riescono a prelevare da quella filiale poiché il denaro contante a portata di mano non è disponibile. Se lo stesso scenario si verifica in più sedi bancarie, la notizia di insolvenza può diffondersi e causare ulteriori prelievi mettendo a rischio una banca di una crisi bancaria sistemica.

bare multisig

Livello: avanzato

Argomento: tecnologia

Nel contesto Bitcoin, bare multisig si riferisce a uno script multifirma che contiene direttamente le chiavi pubbliche coinvolte nella transazione multisig.
Ciò contrasta con il multisig pay-to-script-hash (P2SH), in cui le chiavi pubbliche non sono direttamente integrate nello script di output ma piuttosto in un output di transazione separato che funge da condizione di hashlock.

Il multisig attualmente può essere eseguito in molti modi, ma prima di p2sh (BIP0013), l'unico modo per eseguire il multisig era il bare multisig, mettere i numerosi pubkey on-chain.

È ancora supportato dai portafogli e dai nodi Bitcoin, ma è considerato meno sicuro e più incline agli attacchi di malleabilità delle transazioni rispetto al multisig P2SH.

Poiché ECDSA non consente realmente di aggregare le chiavi, gli output dovevano specificare qualcosa come "3 su 5 di questi pubkey". I normali UTXO hanno il seguente numero di byte:

- p2pkh:25
- p2sh:23
- p2wpkh:22
- p2wsh:34
- p2tr:34

Al contrario, la n nel bare multisig k-of-n determina il numero di byte ed è 5 + 34 * n (più o meno). Quindi per 3 su 5 sono più di 170 byte. Ma questo sta usando chiavi compresse. Per le chiavi non compresse, è 5 + 66 * n o 335 byte+ e, peggio ancora, puoi inserire chiavi non compresse illegittime (chiavi che probabilmente non hanno una chiave privata) per aggiungere dati alla catena

Perché è importante? Perché questi byte rimangono nel set UTXO, che è ciò per cui il software Bitcoin ottimizza perché è così che confermi che una transazione non è una double spend e soddisfa le condizioni dello smart contract che l'ha bloccata.

Quel che è peggio, se le pubkey non sono spendibili (chiavi non compresse che non sono punti reali sulla curva secp256k1), allora non verranno mai prunate. Quindi l'UTXO Set diventa più grande e richiede più risorse rispetto ad un normale nodo.

È interessante notare che questo è il modo in cui il whitepaper è stato incorporato nella blockchain di Bitcoin inserendo pezzi del pdf del whitepaper in blocchi da 64 byte attraverso pubkey non compressi.

Base Fee

Livello: avanzato

Argomento: tecnologia

La base_fee è una impostazione delle fee nei nodi Lightning Network.

È una somma fissa che viene addebitata per ogni inoltro, in genere 1 satoshi.

È possibile impostare una fee base più alta o pari a 0 e addirittura è promossa come buona norma dall'iniziativa Zero Base Fee per per migliorare le prestazioni di Lightning Network.

È anche possibile addebitare qualsiasi importo di millisatoshi.

Poiché ogni inoltro costa in termini di potenza di calcolo e di memoria, la base_fee ha lo scopo di compensare gli sforzi compiuti per inoltrare un pagamento.

Ad esempio, per ogni nuovo stato del canale il nodo deve tenere in archivio una nuova chiave di revoca. Se si utilizza una watchtower, queste informazioni

devono essere inviate e memorizzate anche sulla watchtower.

Tali informazioni devono essere conservate fino alla chiusura del canale, il che può essere costoso.

Base32

Livello: avanzato

Argomento: tecnologia

La codifica base32 è una tecnica di codifica dei dati che utilizza 32 caratteri per rappresentare le informazioni in modo che possano essere trasmesse o memorizzate in modo efficiente. La codifica base32 viene spesso utilizzata per la trasmissione di dati in ambienti in cui è presente un alto tasso di errore, come ad esempio in reti wireless o in sistemi di trasmissione dei dati a lunga distanza.

La codifica base32 utilizza un insieme di 32 caratteri per rappresentare i dati. Questi caratteri sono tutte le lettere dell'alfabeto inglese, senza distinzione tra maiuscole e minuscole, più le cifre da 0 a 9. Ogni carattere rappresenta una combinazione di 5 bit di dati. Ad esempio, il carattere "A" rappresenta i bit "00000", mentre il carattere "Z" rappresenta i bit "11010".

La codifica base32 è simile alla codifica base64, che utilizza 64 caratteri per rappresentare i dati, ma è meno efficiente in termini di spazio. Tuttavia, la codifica base32 ha il vantaggio di essere più facile da digitare e da leggere a occhio nudo, rendendola particolarmente adatta per l'utilizzo in ambienti in cui gli errori sono comuni. Ad esempio, gli indirizzi Bech32m per la rete Lightning di Bitcoin utilizzano la codifica base32 per garantire la sicurezza e l'affidabilità delle transazioni sulla rete.

Base58

Livello: avanzato

Argomento: tecnologia

Base58 è un vecchio formato di codifica utilizzato per rappresentare gli indirizzi Bitcoin noti anche come legacy. Questo schema di codifica si basa su un alfabeto composto da 58 caratteri, includendo sia lettere maiuscole che minuscole dalla A alla Z e le cifre da 1 a 9 ma esclude deliberatamente lo zero, la "O" maiuscola, la "I" maiuscola e la "l" minuscola per evitare possibili confusioni nel lettore.

Una variante di Base58, denominata Base58Check, è ampiamente utilizzata per rappresentare gli indirizzi Bitcoin legacy e le chiavi private in formato Wallet Import Format (WIF).
Base58Check mantiene la struttura di Base58 ma introduce un checksum di 4 byte e un prefisso di versione. Il checksum contribuisce alla sicurezza verificando l'integrità dei dati codificati, mentre il prefisso di versione specifica il tipo di dati rappresentati.

Nel contesto degli indirizzi Bitcoin, il prefisso di versione assume un ruolo cruciale nell'identificare la natura dei dati:

- "1": gli indirizzi Pay-to-Public-Key-Hash (P2PKH) sono caratterizzati da un prefisso "1"
- "3": gli indirizzi Pay-to-Script-Hash (P2SH) presentano il prefisso "3"
- "5": Le chiavi private in formato WIF sono precedute dal prefisso "5"

Questo sistema di prefissi consente agli utenti di distinguere rapidamente il tipo di informazioni rappresentate, contribuendo all'efficienza e alla sicurezza nell'utilizzo di tali dati critici nel contesto delle transazioni e della gestione delle chiavi private.

Base64

Livello: avanzato

Argomento: tecnologia

Base64 è uno schema di codifica usato per codificare le transazioni PSBT (Partially Signed Bitcoin Transaction).
Base64 utilizza un alfabeto di 64 caratteri, comprese tutte le lettere maiuscole e minuscole, le cifre 0-9, e i caratteri '+' e '/'.
A causa del suo lungo alfabeto, Base64 può visualizzare i dati in modo efficiente, ma è meno leggibile. Così, Base64 è usato per codificare dati che non sono spesso letti o trasmessi da esseri umani.

Basket

Paniere

Livello: intermedio

Argomento: finanza

Un paniere di valute, in ambito cripto, è in genere un pool di risorse del mondo reale tokenizzate come materie prime, obbligazioni, titoli e stablecoin che rappresentano valute legali. Inoltre, nello spazio blockchain un paniere di valute è solitamente costituito da Bitcoin, Ethereum e altre criptovalute a grande capitalizzazione. Nella finanza tradizionale un paniere di valute è semplicemente una raccolta di più azioni o titoli che spesso provengono dalle stesse classi di attività o simili. Questi panieri possono essere utilizzati per la negoziazione di derivati e per la funzione di strumenti finanziari e sono spesso gestiti da fondi di investimento istituzionali, hedge fund, fondi comuni di investimento ed Exchange Traded Fund (ETF).

Batching

Livello: avanzato

Argomento: tecnologia

La pratica di combinare più pagamenti bitcoin in un'unica transazione con più output, abbassando così la quantità di dati elaborati e conseguentemente le fee necessariePayment batching, il batching dei pagamenti è la tecnica di includere più pagamenti nella stessa transazione on-chain. Ciò consente di dividere il costo di creazione di una transazione, della spesa degli input e della creazione di un output di cambio tra tutti i pagamenti nella transazione, riducendo il costo medio per pagamento.

È realisticamente possibile risparmiare il 75% sulle commissioni di transazione raggruppando solo un piccolo numero di pagamenti e senza alcuna degradazione della velocità di conferma o altre modifiche necessarie. Anche utilizzando esattamente gli stessi input che utilizzeresti senza il batching, è possibile risparmiare oltre il 20%.

Bear Market

Mercato ribassista

Livello: intermedio

Argomento: finanza

Il Bear Market, raramente tradotto in italiano in Mercato Orso e pià generalmente in Mercato rialzista, si riferisce a un andamento negativo dei prezzi di un mercato.

È ampiamente utilizzato non solo nello spazio delle criptovalute, ma anche nei mercati tradizionali, come azioni, obbligazioni, immobili e mercati delle materie prime. In generale, un mercato ribassista si riferisce a una forte tendenza al ribasso del mercato che presenta prezzi in calo significativo in un periodo di tempo relativamente breve.

Rispetto ai mercati tradizionali, i mercati delle criptovalute sono più piccoli e quindi più volatili. Pertanto, è abbastanza comune vedere mercati ribassisti cripto più forti e prolungati, dove i cali di prezzo dell'85% non sono così rari.

Per Bitcoin, i Bear Market più lunghi possono essere così identificati (i valori sono approssimati):

giorni	dal		al	prezzo iniziale	prezzo finale	drawdown
400	nov 2021	-	nov 2022	$69'000	$15'700	-76%
360	dic 2017	-	dic 2018	$19'800	$3'100	-84%
400	dic 2013	-	gen 2015	$1'240	$150	-87%
160	giu 2011	-	nov 2011	$31	$2	-93%

L'opposto del Bear Market è il Bull Market.

Bear Trap

Trappola per speculatori ribassisti

Livello: intermedio

Argomento: finanza

La Bear Trap è una tecnica che può essere utilizzata da un gruppo di traders, finalizzata a manipolare il prezzo di una criptovaluta.

La Bear Trap viene impostata vendendo in un certo momento una grande quantità di una specifica criptovaluta, facendo credere al mercato che ci sia un imminente calo dei prezzi. In risposta, altri trader vendono i propri asset, abbassando ulteriormente il prezzo. Coloro che impostano la trappola quindi la rilasciano, riacquistando le proprie risorse a un prezzo inferiore. Il prezzo poi rimbalza, permettendo loro di realizzare un profitto.

Può essere il preludio a una short-squeeze, una bear trap è una forma di vendita coordinata ma controllata per creare un calo temporaneo dei prezzi di un asset. Il più delle volte, i trader alle prime armi vengono attratti dalla volatilità dei prezzi quando fanno trading in mercati che si occupano di criptovalute ma o altri asset. Le inversioni di prezzo possono lasciare perplessi anche i trader più esperti, ed è importante identificare i segnali di una falsa inversione, un momentaneo cambiamento nella direzione del prezzo, prima di riprendere il trend sottostante per evitare di caderne preda. L'aumento della volatilità può persino indurre i trader a breve termine a fare più operazioni nel tentativo di prendere la misura dei mercati, provocando perdite profonde per la maggior parte delle persone e con un impatto sulla loro fiducia o convinzione nell'attività sottostante. In un mercato che tende al rialzo, un improvviso movimento al ribasso in termini di prezzi può indurre una maggiore volatilità e potrebbe costringere i partecipanti al mercato a liquidare le partecipazioni a lungo termine o ad andare short sull'attività sottostante nella speranza di guadagnare rapidamente. Questa inversione, se causata da un gruppo di investitori che movimenta grandi importi, può essere temporanea e durare solo per il tempo necessario per riacquistare le proprie partecipazioni a un prezzo inferiore. Chiamata bear trap, questa forma di manipolazione del mercato inganna i partecipanti ribassisti facendogli credere che l'inversione di prezzo indichi l'inizio di una tendenza al ribasso ed è spesso seguita da una brusca ripresa della precedente tendenza al rialzo.

Lo shorting, la pratica di vendere un asset per riacquistarlo successivamente a un prezzo inferiore è di natura estremamente speculativa durante tali periodi di volatilità e porta i trader ribassisti ad assumersi livelli di rischio estremi. Poiché una bear trap è spesso improvvisa e di breve durata, anche gli investitori a lungo termine potrebbero cedere alla pressione di vendita temporanea e perdere parte o tutti i loro profitti.

Simile nel meccanismo visto con altre classi di attività, una bear trap nei mercati delle criptovalute attira scommesse sia ribassiste che rialziste, spesso con rischi

sproporzionati. Usata per descrivere sia il meccanismo che l'inversione di prezzo di breve durata indicando falsamente l'inizio di una tendenza al ribasso, una bear trap nei mercati delle criptovalute è una forma di manipolazione del mercato determinata dagli sforzi concertati di un gruppo di trader che detengono enormi quantità di la criptovaluta sottostante, chiamati whale (balene). Coordinandosi tra loro, la vendita collettiva di un particolare token fa scendere il suo prezzo e influenza gli altri partecipanti al dettaglio a credere che il trend rialzista sia terminato. Di conseguenza, molti investitori possono vendere le proprie partecipazioni e ciò si traduce in un ulteriore calo del prezzo per alcune ore o giorni alla fine. Di solito, quando si rompono al di sotto dei minimi precedentemente mantenuti, questi influenti gruppi di trader procederanno quindi a riacquistare le quantità vendute a prezzi bassi, e questo innesca un forte movimento al rialzo che intrappola le scommesse ribassiste in massa. Nel tentativo di limitare le loro perdite, i trader con posizioni short si affretterebbero quindi ad acquistare la criptovaluta e lo slancio di acquisto risultante serve solo a portare il prezzo ancora più in alto. Pertanto, vendendo a un prezzo più alto e riacquistando tutte le posizioni vendute a un livello di prezzo più basso, il gruppo di trader o i bear trap setters intendono trarre profitto dalla differenza senza influire sulla quantità di criptovaluta da loro detenuta a lungo termine.

Differenze tra Bear trap e short selling La short-selling di una criptovaluta o la creazione di posizioni short attraverso altri strumenti di mercato è un precursore della formazione di una bear trap. Come con altre classi di attività, le criptovalute popolari come Bitcoin possono essere shortate utilizzando diversi meccanismi come token di short-selling, trading a margine o trading di futures e opzioni della criptovaluta di base. Queste strade sono spesso utilizzate da trader esperti e investitori istituzionali per coprire le proprie posizioni nel mercato secondario e possono proteggere i propri investimenti in caso di inversione di tendenza del mercato. In quanto tale, la short-selling di una criptovaluta o lo shorting con uno qualsiasi dei mezzi disponibili è una pratica comune, ma avviene in volumi che sono una frazione del volume di scambio di token primario. Tuttavia, se fatto su scala eccessivamente ampia, lo shorting di una criptovaluta come BTC può creare un'immensa pressione al ribasso sui suoi prezzi a causa di un aumento collettivo del quoziente di paura. Indicatori tecnici come l'indice di forza relativa (RSI relative strength index) possono alludere a una criptovaluta che entra in territorio ribassista, che può quindi innescare una più ampia svendita guidata da investitori retail meno informati che vogliono togliersi di mezzo il rischio. Se questo sentimento si mantiene e i prezzi scendono al di sotto dei livelli di supporto chiave, può indurre ancora più investitori ribassisti ad andare short per fungere da opportunità redditizia per le grandi entità commerciali causando una sbear rhort coprendo le loro posizioni short originali. Pertanto, una bear trap è preceduta dalla short-selling di una criptovaluta da parte di un gruppo di investitori che hanno grandi partecipazioni in token e terminano quando chiudono le loro posizioni in derivati, riacquistano le loro posizioni in criptovaluta vendute allo scoperto o una combinazione di entrambi. Sebbene

chiunque possa aprire una posizione short o short-sell una criptovaluta, la collusione con altri partecipanti per manipolare il prezzo di un asset è considerata illegale in mercati come gli Stati Uniti e può suscitare l'ira di varie autorità centrali.

Come identificare ed evitare una bear trap? Una bear trap può essere riconosciuta utilizzando gli strumenti grafici disponibili sulla maggior parte delle piattaforme di trading e richiede cautela da esercitare.

Nella maggior parte dei casi, l'identificazione di una bear trap richiede l'uso di indicatori di trading e strumenti di analisi tecnica come RSI, livelli di Fibonacci e indicatori di volume, ed è probabile che confermino se l'inversione di tendenza dopo un periodo di costante movimento al rialzo dei prezzi è genuina o intendeva semplicemente invitare degli short.

Qualsiasi tendenza al ribasso deve essere guidata da elevati volumi di scambio per escludere la possibilità che sia stata messa in atto una bear trap. In generale, una combinazione di fattori, tra cui il ritracciamento del prezzo appena al di sotto di un livello di supporto chiave, la mancata chiusura al di sotto dei livelli critici di Fibonacci e bassi volumi, sono segni di una bear trap.

Per gli investitori in criptovalute con una bassa propensione al rischio, è meglio evitare di fare trading durante inversioni di prezzo brusche e infondate a meno che l'azione di prezzo e volume non confermi un'inversione di tendenza al di sotto di un importante livello di supporto.

Ha senso mantenere le partecipazioni in criptovaluta durante tali periodi ed evitare di vendere a meno che i prezzi non abbiano violato il prezzo di acquisto iniziale o il livello di stop loss. È utile capire come le criptovalute e l'intero mercato delle criptovalute reagiscono alle notizie, ai sentimenti o persino alla psicologia della folla.

Praticare questo può essere molto più difficile di quanto sembri, soprattutto quando si tiene conto dell'elevata volatilità associata alla maggior parte delle criptovalute che attualmente vengono scambiate.

D'altra parte, se si vuol trarre profitto dall'inversione del momentum, è meglio entrare in un'opzione put piuttosto che fare short selling o diventare un venditore short nella criptovaluta sottostante. Questo perché lo short selling o la vendita di una call può esporre il trader a rischi illimitati se la criptovaluta riprende la sua tendenza al rialzo, il che non è il caso se si opta per una posizione put. In quest'ultima strategia, le perdite sono limitate al premio pagato e non hanno alcuna influenza su eventuali posizioni long in criptovalute detenute da prima. Per gli investitori a lungo termine che cercano profitto senza rischi elevati, è meglio evitare del tutto il trading durante una bear trap.

Bearish

Livello: intermedio

Argomento: finanza

Indica un trend ribassista, vedi Bear Market.

In generale Bearish, o ribassista in italiano, si riferisce a un atteggiamento o a una prospettiva che prevede un calo dei prezzi.

Nel mercato delle criptovalute, una persona che è Bearish su una determinata criptovaluta o sul mercato delle criptovalute in generale, crede che i prezzi scenderanno in futuro.

In sintesi, un investitore bearish si aspetta un calo dei prezzi delle criptovalute, per questo è più propenso a vendere o shortare (cioè speculare sulla discesa dei prezzi) le criptovalute invece che comprarle.

Questo atteggiamento è contrario a quello di una persona che è Bullish e crede che i prezzi saliranno.

Bech32

Livello: avanzato

Argomento: tecnologia

Bech32 è un formato di indirizzo Bitcoin completamente compatibile con SegWit.

Questo formato di indirizzo è noto anche come **indirizzi bc1** perché le loro stringhe di indirizzo bitcoin iniziano sempre con bc1. Questo nuovo tipo di indirizzo apporta alla rete Bitcoin maggiore efficienza e riduce le commissioni delle transazioni nell'invio di BTC da un indirizzo all'altro. Una stringa Bech32 è lunga al massimo 90 caratteri ed è composta da:

La parte leggibile dall'uomo:

- **bc** per mainnet
- **tb** per testnet

Il separatore, che è sempre **1**.

La parte dati, che è lunga almeno 6 caratteri e consiste solo di caratteri alfanumerici esclusi "1", "b", "i" e "o".

È stato introdotto con la BIP 173.

Con l'aggiornamento Taproot, viene proposta la variante Bech32m, a causa di una vulnerabilità nel bech32.

L'indirizzo Bech32 è un formato di indirizzo utilizzato per ricevere o inviare pagamenti sulla blockchain di Bitcoin. È stato sviluppato come un'alternativa più sicura e affidabile al formato di indirizzo base58 utilizzato nei normali indirizzi Bitcoin.

Gli indirizzi Bech32 sono composti da una stringa di caratteri alfanumerici che inizia con "bc1" seguita da una serie di caratteri separati da trattini. Ad esempio, un indirizzo Bech32 potrebbe essere bc1qw508d6qejxtdg4y5r3zarvary0c5xw7kv8f3t4.

Il formato Bech32 utilizza una codifica di tipo base32 che è più resistente agli errori rispetto alla codifica base58 utilizzata negli indirizzi Bitcoin Legacy. Inoltre, gli indirizzi Bech32 includono un codice di controllo che consente di verificare l'integrità dell'indirizzo durante la trasmissione.

Gli indirizzi Bech32 sono stati introdotti per la prima volta nella versione 0.16.0 del software Bitcoin Core nel 2018. Oggi sono supportati quasi tutti i wallet e dagli Exchange Bitcoin. Tuttavia, alcuni wallet molto vecchi potrebbero non supportare ancora gli indirizzi Bech32, quindi è sempre importante verificare che l'indirizzo che si sta utilizzando sia supportato dallo strumento o servizio che si sta utilizzando.

Bech32m

Livello: avanzato

Argomento: tecnologia

Bech32m è il formato di indirizzi introdotto con l'aggiornamento Taproot.

Bech32m è una versione modificata dello schema di codifica Bech32, utilizzato per codificare gli indirizzi SegWit. Bech32m è quasi identico a Bech32: Utilizza una codifica di tipo base32 che è più resistente agli errori rispetto alla codifica base58 utilizzata nei normali indirizzi Bitcoin.; usa solo lettere minuscole; e inizia con una parte leggibile dall'uomo, che è "bc1" per gli indirizzi SegWit. Bech32 ha un meccanismo di rilevamento degli errori integrato, che ha lo scopo di rilevare alterazioni ai dati codificati da Bech32.

Tuttavia, l'implementazione originale di Bech32 presentava una vulnerabilità in questo meccanismo, che consentiva a un utente malintenzionato di modificare un indirizzo senza invalidare il checksum.

Quando una stringa Bech32 termina con una "p", l'aggiunta o la rimozione di "q" prima della "p" non la invalida. Bech32m rimuove questa vulnerabilità modificando una costante utilizzata nello schema di codifica, ed è quindi più sicuro.

Come specificato in BIP 350 come schema di codifica per gli indirizzi SegWit versione 1 (Taproot).

Benchmark

Livello: intermedio

Argomento: finanza

Benchmark o Benchmarking è un metodo per confrontare la performance di un asset o portafoglio di investimenti con quella di asset simili per vedere se c'è un divario che può essere colmato aumentando gli indicatori di performance. Un benchmark index, o indice di riferimento, si riferisce a un titolo indice preminente utilizzato come misura, o benchmark, rispetto al quale è possibile monitorare le prestazioni del mercato più ampio. Gli indici di riferimento comuni includono S&P 500, Nasdaq Composite e Russell 3000.

BFA

Acronimo di: Brute Force Attack

Livello: intermedio

Argomento: tecnologia

Il Brute Force Attack, o attacco a forza bruta, è un metodo per tentare di decifrare una password, una chiave crittografica o un dato semplicemente tenando ogni possibile password o chiave di decifrazione tra le possibili combinazioni. L'attacco a forza bruta è altamente inefficiente, quindi di solito viene utilizzato come ultima risorsa contro un sistema che non è in grado di resistere ad altri metodi di attacco più efficienti.

Nel contesto della crittografia, un problema o un calcolo è considerato "difficile" se il miglior metodo possibile per risolverlo è un attacco a forza bruta. Questo perché l'attacco a forza bruta viene solitamente utilizzato solo quando nessun algoritmo o altro metodo è in grado di risolvere il problema.

La difficoltà di un BFA può essere calcolata semplicemente prendendo il numero di valori validi - di solito uno solo - e dividendolo per il numero di valori possibili. Ad esempio, una chiave privata Bitcoin è solitamente lunga 256 bit. Il tempo necessario per indovinare una password cresce in modo esponenziale (e non lineare) al crescere della lunghezza della password. Per questo motivo, la dimensione dei bit delle chiavi crittografiche è aumentata gradualmente, passando da uno standard iniziale di 56 bit fino allo standard moderno di 128 o 256 bit. Per forzare una specifica chiave privata Bitcoin con il BFA, un aggressore dovrebbe indovinare correttamente ciascuno dei 256 bit che la compongono, e poiché ogni bit ha due valori possibili (1 o 0), l'aggressore deve indovinare da una gamma di 2^256 (circa 10^77) valori possibili. In confronto, un numero di carta di credito di 16 cifre più un codice di sicurezza di 3 cifre ha una gamma di 10^19 possibilità. Questo uno degli elementi che rende Bitcoin molto più sicuro dei sistemi finanziari tradizionali.

La maggior parte dei sistemi che richiedono password chiede agli utenti di includere lettere maiuscole, numeri e caratteri speciali per ridurre l'efficacia degli attacchi brute force. Questo funziona perché maggiore è il numero di password possibili, più difficile è il BFA.

I BFA prevedono l'uso di un software complesso per inondare un sistema con

ogni potenziale password o chiave al fine di trovare il valore corretto. In teoria, un attacco di questo tipo potrebbe essere utilizzato per indovinare qualsiasi password o chiave e ottenere l'accesso ai dati crittografati. La quantità di tempo teorica necessaria per il successo di un attacco di forza bruta è utilizzata come misura chiave della forza di un sistema di crittografia. Le risorse necessarie per condurre con successo un attacco di forza bruta su un sistema ben protetto sono considerevoli. I supercomputer stessi richiedono condizioni ambientali estremamente controllate e hanno requisiti energetici molto elevati. Le moderne GPU e l'hardware dedicato noto come ASIC - entrambi molto diffusi - si prestano molto bene alle operazioni di violazione delle password e sono accessibili praticamente a chiunque.

Piuttosto che l'uso della forza bruta, l'accesso illegittimo ai sistemi che utilizzano questo tipo di protezione si basa generalmente sullo sfruttamento di un errore umano nell'implementazione del sistema.

Esistono delle specializzazioni degli attacchi rispetto al Brute Force, ad esempio il Dictionary che si basa appunto su dizionario dei valori più utilizzati, o effettuando dei tentativi con password comunemente utilizzate o con combinazioni di lettere e numeri. Anche se i BFA possono essere intensivi dal punto di vista computazionale, richiedono molto tempo e sono difficili da portare a termine, possono indovinare correttamente una password debole in pochi secondi. Una password forte può scoraggiare la maggior parte dei BFA.

BFT

Acronimo di: Byzantine Fault Tolerance

Livello: avanzato

Argomento: tecnologia

La Byzantine Fault Tolerance (BFT) è la proprietà di un sistema informatico che gli permette di raggiungere il consenso nonostante il fallimento di alcuni dei suoi componenti.
La BFT è una caratteristica dei sistemi decentralizzati e permissionless che consente di identificare e rifiutare con successo informazioni disoneste o difettose. I sistemi con tolleranza ai guasti bizantini si basano sulla risoluzione del problema dei generali bizantini e sono in grado di resistere ai Sybil attack.

In un sistema decentralizzato e permissionless, chiunque può unirsi alla rete e iniziare a trasmettere informazioni. Senza la Byzantine Fault Tolerance, qualsiasi membro della rete potrebbe fornire informazioni non valide e minare l'affidabilità del sistema. Nel contesto di Bitcoin, un nodo può facilmente unirsi alla rete e iniziare a trasmettere blocchi e transazioni. Ad esempio, un nodo potrebbe trasmettere due transazioni spendendo lo stesso bitcoin, ovvero effettuare una doppia spesa. Pertanto, Bitcoin ha bisogno di un modo per i nodi di determinare la validità dei dati che ricevono.

Bitcoin è Byzantine Fault Tolerant perché ogni nodo può verificare indipendentemente e oggettivamente ogni transazione e blocco. Se un nodo trasmette blocchi o transazioni non validi, tutti gli altri nodi li riconosceranno e li rifiuteranno, impedendo alle transazioni non valide di entrare nella blockchain. Le regole di Bitcoin sono oggettive, poiché la validità delle transazioni e dei blocchi non è mai ambigua.

Bid-Ask Spread

Spread denaro-lettera

Livello: intermedio

Argomento: finanza

Uno spread Bid-Ask è la differenza tra il prezzo di acquisto di un bene e il prezzo di vendita di quel bene. Bit (offerta) è il prezzo più alto che qualcuno è disposto a pagare per un'attività in un particolare mercato. Ask (richiesta) è il prezzo più basso che qualcuno è disposto a ricevere per vendere un'attività in quello stesso mercato. Uno spread Bid-Ask è sempre presente nei mercati dei capitali, poiché il prezzo al quale si può vendere un'attività sarà sempre inferiore al prezzo al quale si può acquistare l'attività.

Sia l'offerta che la richiesta saranno ordini di maker. Se un ask e un bid si sovrappongono, il risultato sarà un'operazione eseguita tra queste parti. Una volta che lo scambio è stato eseguito, questi ordini vengono rimossi e il mercato ha un nuovo bid-ask spread.

BIP

Acronimo di: Bitcoin Improvement Proposal

Livello: avanzato

Argomento: tecnologia

Per far evolvere il protocollo Bitcoin, la comunità deve predisporre proposte sotto forma di documenti tecnici, noti come Bitcoin Improvement Proposals (BIP), e presentarli alla valutazione, discussione e approvazione della comunità Bitcoin. Questo processo di miglioramento del protocollo Bitcoin è essenziale per assicurare che il sistema rimanga al passo con i cambiamenti del mercato e le esigenze degli utenti.

Le proposte di miglioramento del protocollo sono numerate progressivamente per consentire una facile identificazione e tracciabilità, e l'adozione di queste migliorie può avere un impatto significativo sul funzionamento del protocollo stesso. In alcuni casi, per poter essere adottate, queste proposte richiedono un forte consenso nella comunità Bitcoin.

Il processo di approvazione di una proposta BIP è generalmente composto da un'analisi tecnica e un periodo di discussione tra i membri della comunità. Se la proposta viene accettata, viene integrata nel codice sorgente del protocollo Bitcoin e diventa parte della versione successiva del software Bitcoin.

Il protocollo Bitcoin è un sistema decentralizzato, quindi l'evoluzione del protocollo deve essere gestita in modo collaborativo, coinvolgendo la comunità di sviluppatori, miner e utenti di Bitcoin. In questo modo, gli aggiornamenti del protocollo diventano una responsabilità collettiva per la comunità, garantendo una maggiore sicurezza e affidabilità del sistema Bitcoin.

Esiste anche un apposito BIP che definisce e documenta tale processo, il BIP-2.

Chiunque può proporre un BIP.
L'autore del BIP è responsabile della costruzione del consenso all'interno della comunità e della documentazione delle opinioni dissenzienti.

In Italia BIP è anche la sigla di Bitcoin Italia Podcast, il podcast settimanale condotto da Rikki e Guybrush che dal 2019 vi portano alla scoperta dell'incredibile mondo del Bitcoin, una tecnologia rivoluzionaria spiegata con parole semplici.

BIP 112 CSV

Acronimo di: Check Sequence Verify

Livello: avanzato

Argomento: tecnologia

CSV (CheckSequenceVerify) è una delle funzioni Locktime di Bitcoin, che consente di impostare quando una transazione possa essere pagata. CSV è un locktime relativo che opera a livello di script. Questo consente di definire il momento esatto in cui terminerà un lock su una determinata transazione e quindi potrà essere pagata.

CSV abilita le funzionalità utili per costruire sistemi basati sui canali di pagamento come Lightnin Network, exchange decentralizzati (DEX).

CSV opera in modo simile a CLTV (CheckLockTimeVerify), in CSV viene controllata la parte superiore dello stack con il campo di input, invece di controllare l'ora come nel caso di CLTV. In questo modo si può calcolare il tempo in base al numero di blocchi che sono stati generati dopo la conferma della transazione. I timelock relativi come CSV possono contrassegnare una transazione come non valida. E per questo monitorano che sia trascorso l'intervallo di tempo stabilito da quando sono stati confermati gli output precedenti della transazione. I timelock relativi ci consentono di definire esattamente il tempo che deve trascorrere prima che una transazione possa essere confermata. A differenza dei timelock assoluti che definiscono il momento esatto (block height o timestamp) in cui terminerà il lock sulla transazione.

BIP 113 Median time-past

Livello: avanzato

Argomento: tecnologia

In un network decentralizzato come Bitcoin non esiste un servizio che fornisce un tempo affidabile: gli eventi non sono simultanei, esiste una latenza nella propagazione delle informazioni tra i partecipanti e ogni nodo ha il suo orario che può essere più o meno preciso. Sono i miner ad inserire il timestamp nei nuovi blocchi da loro minati e su questo hanno un certo grado di libertà, e ci sono diversi blocchi nella blockchain bitcoin nei quali blocchi successivi hanno un orario inferiore a quelli precedenti. Inoltre dal momento che le regole del consenso non impongono un rigoroso ordinamento dei timestamp dei blocchi, si crea un incentivo perverso per i miner nel poter impostare ad arte il timestamp nei nuovi blocchi minati al fine di riscuotere fee più sostanziose includendo transazioni che potrebbero non essere ancora valide, transazioni che hanno un timelock che ancora non è passato.

BIP-113 definisce una nuova misurazione del consensus time, l'orario concordato tra i partecipanti alla rete, chiamata Median time-past: viene calcolato prendendo il timestamp degli ultimi 11 blocchi e facendo la media, e utilizzare per i timelock questo orario medio invece del timestamp deciso dal miner del blocco nel quale è inserita la transazione. Le regole di consenso esistenti garantiscono che questo valore avanzi in modo monotono, eliminando così la possibilità per i miner di inserire transazioni ancora bloccate con fee alte impostando dei timestamp artefatti. Median time-past cambia l'implementazione del calcolo del tempo per nLocktime, CLTV, nSequence e CSV (il consensus time è approssimativamente un'ora indietro rispetto all'orologio). Se si creano transazioni con timelock occorre tenerne conto quando si stima il valore desiderato da codificare in nLocktime, CLTV, nSequence e nSequence.

BIP 118 (ANYPREVOUT)

Livello: avanzato

Argomento: tecnologia

Anyprevout, a volte abbreviato con la sigla APO, è un modo per rendere più flessibile la creazione di transazioni Bitcoin.

In una transazione Bitcoin normale, è necessario specificare esattamente quale output precedente si vuole utilizzare come input in ingresso. Con Anyprevout, invece, è possibile firmare una transazione senza fare riferimento ad un output specifico in ingresso e poi aggiungere dinamicamente qualsiasi output con la firma corrispondente in un secondo momento. Ciò significa che è possibile creare transazioni più flessibili, indicando ad esempio dove si vuole ricevere il pagamento e poi rendere disponibile questa transazione a chi può e vuole completandola indicando da dove vengono presi i fondi da trasferire.

BIP-118 SIGHASH_ANYPREVOUT (chiamata in precedenza SIGHASH_NOINPUT) è la proposta di soft-fork che consente di firmare una transazione senza fare riferimento a uno specifico output precedente. Qualsiasi output con una firma corrispondente può essere aggiunto dinamicamente in seguito.

È stata implementata nella testnet da dicembre 2022.

SIGHASH_ANYPREVOUT è un nuovo tipo di Sighash flag: i Sighash flag si trovano all'interno delle transazioni Bitcoin per indicare quale parte della transazione è firmata esattamente dalle chiavi private richieste. Può trattarsi di (quasi) l'intera transazione o di parti specifiche di essa. Firmare solo parti specifiche consente una certa flessibilità nel modificare la transazione anche dopo che è stata firmata, cosa che a volte può essere utile.

Con questa proposta, Sighash flag Anyprevout firma la maggior parte della transazione, ma non gli input. Ciò significa che gli input possono essere scambiati, purché i nuovi input siano ancora compatibili con la firma.

Un uso potenziale può essere relativo ai protocolli off-chain come Lightning Network che sono basati sullo scambio di transazioni che non vengono trasmesse subito alla rete Bitcoin per rinegoziare lo stato finale che dovrebbe essere regolato on-chain.

In alcuni casi si può voler rispondere a una determinata transazione che viene vista on-chain con una reazione predeterminata sotto forma di un'altra transazione.

Spesso questa risposta può essere richiesta per una serie di transazioni diverse che vengono viste on-chain, ma poiché le firme di input nella transazione di risposta sono vincolate a fare riferimento all'esatta transazione a cui si sta reagendo, ciò significa che deve essere creata una nuova firma per ogni possibile transazione a cui si desidera essere in grado di reagire.

La BIP 118 introduce un nuovo tipo di chiave pubblica che modifica il comportamento dell'algoritmo di digest delle transazioni utilizzato nella creazione e nella verifica della firma, escludendo il commitment nei confronti dell'output precedente (e, opzionalmente, del witness script e del valore). L'eliminazione di questo commitment consente il rebinding dinamico di una transazione firmata a un altro output precedente che richiede l'autorizzazione della stessa chiave.

Il rebinding dinamico è opt-in a causa dell'utilizzo di un tipo di chiave pubblica separata, e l'ampiezza delle transazioni a cui la firma può essere legata (rebound) può essere ulteriormente limitata utilizzando chiavi diverse, effettuando il commitment sullo script che viene speso nella firma, utilizzando importi diversi tra gli UTXO, utilizzando valori diversi di nSequence nella transazione di spesa, o utilizzando l'opcode codeseparator per impegnarsi sulla posizione nello script.

Per la proposta di layer Eltoo per Lightning Network è necessario un sighash di tipo noinput.

BIP 119 (CTV)

Acronimo di: Check Template Verify

Livello: avanzato

Argomento: tecnologia

CheckTemplateVerify (CTV) è una proposta soft fork per Bitcoin specificata nella Bitcoin Improvement Proposal (BIP) 119.
Mira a consentire nuovi casi d'uso per la rete aggiungendo un tipo di base o smart contract di covenant (patto).

CTV consente a un utente Bitcoin di limitare il modo in cui può spendere bitcoin anche se ha la chiave del bitcoin che desidera spendere.
Ancora più importante, CTV consente di applicare queste restrizioni alla spesa in modo non interattivo. Alcuni casi d'uso abilitati da CTV potrebbero essere resi possibili oggi, ma il più delle volte l'insieme di utenti che partecipano all'accordo di smart contract dovrebbe essere online e interagire manualmente per coordinare le regole di spesa, il che non è sempre possibile. CTV consente di applicare queste restrizioni in modo programmatico, senza richiedere l'interazione manuale dei partecipanti, aumentando così l'affidabilità del patto.

Oggi puoi spendere i tuoi UTXO come vuoi. In un mondo post-CTV, potresti mettere in atto regole sui tuoi UTXO per controllare o limitare i possibili modi in cui potresti spendere quelle monete. Non quando sono spesi, ma come.
Introducendo questi tipi di nuove funzionalità in Bitcoin, potrebbe essere abilitato un insieme più diversificato di casi d'uso e potrebbe emergere un nuovo ecosistema di applicazioni.

L'adozione di CTV è controversa perché potrebbe minacciare la fungibilità dei Bitcoin, poiché aggiunge la possibilità di inserire dei vincoli sulla destinazione di un determinato ammontare di Bitcoin, impedendo la loro spesa verso qualsiasi altro indirizzo.

BIP 125 (RBF)

Acronimo di: Replace-by-Fee

Livello: avanzato

Argomento: tecnologia

BIP 125 definisce le caratteristiche per la funzione RBF Replace-by-Fee in Bitcoin. Questo soft fork consente agli utenti di sostituire una transazione non confermata con una transazione simile pagando fee (commissione) più alte.

Alcuni wallet Bitcoin, come Bitcoin Core, Blockstream Green, Electrum, Samourai Wallet, Specter Wallet, SBW Simple Bitcoin Wallet, Moonshine, Coinb.in, ConIO, Nunchuk, consentono agli utenti di utilizzare RBF.

Quando una transazione viene trasmessa, paga una fee definita al miner per inserire la transazione in un blocco della blockchain.

I miner, che guadagnano anche sulle fee, preferiscono riempire i blocchi con le transazioni che hanno le fee più alte, e se la transazione ha una fee più bassa delle altre transazioni, dovrà aspettare più tempo prima di essere inserita nel blocco.

Al fine di accelerare la conferma di una transazione, ovvero l'inserimento in un nuovo blocco della blockchain, un utente può sfruttare RBF per aumentare le fee della propria transazione.

I nodi che seguono BIP 125 accetteranno la nuova transazione e rimuoveranno la versione precedente dal loro mempool.

Prima di BIP 125, i nodi Bitcoin rifiutavano automaticamente una transazione che tentava di spendere UTXO già spesi in una transazione diversa nella loro mempool.

BIP 125 ha creato un modo per intervenire su tale regola. Tuttavia, una transazione deve attivare RBF nella sua prima versione per rendere possibile RBF. Questo viene fatto utilizzando nSequence, un campo precedentemente inutilizzato di un input di transazione.

BIP 129 (BSMS Bitcoin Secure Multisig Setup)

Livello: avanzato

Argomento: tecnologia

L'esperienza del multisig di Bitcoin è stata notevolmente semplificata da BIP-0174 (transazione Bitcoin parzialmente firmata).

Tuttavia, manca ancora un processo standardizzato per la creazione di wallet multisig in modo sicuro tra i diversi fornitori.

Quando si tratta di configurare un wallet multisig, le preoccupazioni sono molteplici:

- La configurazione del multisig, come l'appartenenza al firmatario, il tipo di script, i percorsi di derivazione e il numero di firme richieste, è corretta e non è stata manomessa.
- Se le chiavi o la configurazione multisig sono trapelate durante la configurazione.
- Se il firmatario conserva la configurazione multisig nella propria memoria e in quale formato.
- Se la memoria del firmatario è a prova di manomissione.
- Se il firmatario utilizza successivamente la configurazione multisig per generare e verificare gli indirizzi di ricezione e modifica.

Un aggressore in grado di modificare la configurazione multisig può rubare o tenere in ostaggio i fondi ingannando l'utente e facendogli inviare i fondi all'indirizzo sbagliato. Un aggressore che non può modificare la configurazione, ma che può conoscere le chiavi e/o la configurazione, può monitorare le transazioni nel wallet, con conseguente perdita di privacy. Questa proposta cerca di risolvere i problemi #1, #2 e #3: mitigare il rischio di manomissione durante la fase iniziale di configurazione e definire un formato di configurazione multisig interoperabile.

I problemi #4 e #5 dovrebbero essere gestiti dai firmatari e non rientrano nell'ambito di questa proposta.

BIP 141 (Segregated Witness)

Livello: avanzato

Argomento: tecnologia

Vedi SegWit

BIP 155 (addrv2 message)

Livello: avanzato

Argomento: tecnologia

Il BIP 155 addrv2 message propone un nuovo messaggio P2P per comunicare indirizzi di nodi più lunghi sulla rete P2P. Ciò è necessario per supportare indirizzi Onion di nuova generazione, I2P e potenzialmente altre reti che hanno indirizzi endpoint più lunghi di quelli che rientrano nei 128 bit del messaggio addr corrente.

I Tor v3 hidden services fanno parte della versione stabile di Tor dalla versione 0.3.2.9. Presentano diversi vantaggi rispetto ai vecchi hidden services, tra cui una migliore crittografia e privacy. Questi servizi hanno indirizzi a 256 bit e quindi non si adattano al messaggio addr esistente, che incapsula gli indirizzi onion negli indirizzi IPv6 OnionCat.

Altri protocolli del livello di trasporto come I2P hanno sempre utilizzato indirizzi più lunghi. Questa modifica consentirebbe di comunicare tali indirizzi sulla rete P2P, in modo che altri peer possano connettersi ad essi.

BIP 158 (Block Filters for Light Clients)

Livello: avanzato

Argomento: tecnologia

I BIP 158 block filters sono un tipo di filtro di blocco che consente ai light client (SPV - Simplified Payment Verification) di Bitcoin di scaricare solo i blocchi che contengono transazioni che li riguardano.

Sono una proposta per migliorare la privacy e l'efficienza dei client leggeri Bitcoin. Furono proposti nel 2016 da Roasbeef e Thrasher. Il loro utilizzo comporta dei miglioramenti in termini di banda e di efficienza rispetto ai Bloom filters (BIP 37).

Questi filtri sono stati proposti per la prima volta nel 2016 con l'intento di migliorare le prestazioni e la privacy dei client leggeri di Bitcoin, sono filtri di tipo Golomb-Rice che permettono di verificare la presenza di determinate transazioni nei blocchi Bitcoin in modo efficiente.

Invece di scaricare l'intera blockchain, un light client che utilizza i BIP 158 block filters può richiedere solo i blocchi che contengono transazioni che lo riguardano, riducendo così il traffico di rete e i tempi di sincronizzazione.

I BIP 158 block filters sono stati implementati in diversi wallet, tra cui Wasabi Wallet.

Come funzionano i BIP 158 block filters? Si basano su un meccanismo di probabilistic filtering, che permette di creare un filtro compatto per ogni blocco, contenente informazioni sulle transazioni al suo interno.
Un nodo completo genera questi filtri e li rende disponibili ai client leggeri.
Un client leggero può scaricare solo il filtro invece di tutto il blocco, verificando se un certo indirizzo o output è presente.
Se un filtro indica la possibile presenza di una transazione di interesse, il client può scaricare solo quel blocco specifico per ulteriori verifiche.

BIP 16 (P2SH)

Acronimo di: Pay-to-Script-Hash

Livello: avanzato

Argomento: tecnologia

BIP 16 ha introdotto gli output Pay-to-Script-Hash (P2SH). Attivato nel 2013, BIP 16 è stato un miglioramento significativo per la flessibilità di Bitcoin, consentendo transazioni multi-firma più economiche e private, una maggiore capacità degli smart contract e retrocompatibilità per SegWit, un aggiornamento che sarebbe arrivato diversi anni dopo.

In base a BIP 16, gli output P2SH bloccano i bitcoin sull'hash di uno script Bitcoin. Per spendere questi bitcoin, è necessario fornire lo script e le eventuali firme necessarie.

Gli indirizzi P2SH utilizzano la codifica Base58 e iniziano con "3".

L'aggiornamento BIP 16 è stato anche oggetto di molte controversie. È stato il primo importante aggiornamento ad essere implementato in Bitcoin dopo che Satoshi Nakamoto, il creatore di Bitcoin, è scomparso e sono state quasi attivate diverse proposte alternative, alcune con difetti critici.

BIP 173 Bech32

Livello: avanzato

Argomento: tecnologia

Con BIP 173 è stato proposto il nuovo formato per gli indirizzi bitcoin chiamato "Bech32" come standard per gli indirizzi SegWit. Il titolo del BIP 173 è "Base32 address format for native v0-16 witness outputs", dove Base32 è il tipo di codifica utilizzato, e con native witness outputs si intendono gli indirizzi nativi SegWit

BIP 174 (PSBT)

Acronimo di: Partially Signed Bitcoin Transaction Format

Formato di transazione Bitcoin parzialmente firmato

Livello: avanzato

Argomento: tecnologia

BIP 174 ha introdotto le transazioni Bitcoin con firma parziale (PSBT). PSBT è un formato standard per la comunicazione di transazioni Bitcoin non firmate o parzialmente firmate.
PSBT è stato originariamente progettato per migliorare l'interoperabilità tra i wallet e altri software Bitcoin, rendendo più semplice la creazione di una transazione da parte di un wallet, il trasferimento a un altro per la firma e quindi il trasferimento a un nodo Bitcoin per la trasmissione.
PSBT è anche particolarmente utile per il coordinamento tra le parti che desiderano firmare la stessa transazione.
Ad esempio, i protocolli CoinJoin e gli output multisig richiedono più attori diversi per firmare tutti la stessa transazione. Il formato PSBT fornisce un metodo per costruire la transazione, passarla tra i diversi firmatari e quindi assemblare la transazione finale da trasmettere. BIP 174 è attualmente ampiamente adottato come standard dalla comunità, tuttavia presenta diversi aspetti negativi, che sono oggetto della una proposta per PSBT v2.

BIP 179 (Name for payment recipient identifiers)

Nome per gli identificatori del destinatario del pagamento

Livello: avanzato

Argomento: tecnologia

La BIP 179 ha lo scopo di proporre un nuovo termine per indirizzo con il termine "invoice" (con il significato in italiano di *richiesta di pagamento*, e non *fattura* che è una delle possibili traduzioni in italiano del termine invoice).

Il termine invoice è quello predefinito ad esempio nel protocollo Lightning ed è in realtà più accurato, dal punto di vista tecnico, perché il termine indirizzo o

address normalmente utilizzato rischia di essere fuorviante a causa delle caratteristiche del termine indirizzo al di fuori del contesto delle criptovalute.

Gli indirizzi Bitcoin sono destinati a essere utilizzati una sola volta e bisognerebbe generarne uno nuovo per ogni nuovo pagamento in entrata. Il termine "indirizzo", tuttavia, indica coerenza, perché quasi tutto ciò che su Internet o nel mondo offline ha il termine "indirizzo" è qualcosa che cambia raramente o addirittura mai (indirizzo postale, indirizzo e-mail, indirizzi IP (dipende molto dal provider), ecc.

BIP 21 (URI scheme)

Livello: avanzato

Argomento: tecnologia

La BIP-21 URI Scheme, è una proposta di miglioramento del protocollo BIP per la creazione di indirizzi Bitcoin in formato URI Uniform Resource Identifier.

Il BIP-21 introduce un formato standard per gli indirizzi Bitcoin in URI, che consente ai wallet e alle altre applicazioni di utilizzare indirizzi Bitcoin in modo più semplice e consistente.

Il formato standard include informazioni come l'indirizzo Bitcoin, l'importo da inviare e un messaggio opzionale. In questo modo, gli utenti possono facilmente inviare bitcoin ad un indirizzo specifico e includere un messaggio di accompagnamento, semplicemente cliccando su un link.

BIP 32 (HD Wallet)

Livello: avanzato

Argomento: tecnologia

BIP 32 ha introdotto lo standard dei wallet Hierarchical Deterministic (HD) e le chiavi estese a Bitcoin.
BIP 32 è stato un miglioramento significativo per i wallet Bitcoin in diversi modi. Innanzitutto, i wallet HD hanno notevolmente migliorato l'interoperabilità dei wallet, poiché un set di chiavi potrebbe essere trasferito tra il software del wallet con una singola chiave privata estesa xprv.

È stata migliorata la gestione del backup e restore dei wallet, poiché un singolo seed potrebbe recuperare l'intero wallet. Questo miglioramento è stato esteso con BIP 39, che ha reso i semi più facili da conservare e ricordare. Infine, BIP 32 ha abilitato i wallet watch-only, in grado di memorizzare e generare nuovi indirizzi, consentendo all'utente di ricevere pagamenti e controllare i propri saldi senza mai dover utilizzare chiavi private.

I wallet Watch-only migliorano la sicurezza di un utente consentendo loro di conservare le proprie chiavi private in Cold storage, continuando a ricevere bitcoin,

tenere traccia dei saldi e creare transazioni.

BIP 34 (Block Height in Coinbase)

Livello: avanzato

Argomento: tecnologia

Il BIP 34, Block Height in Coinbase ovvero Altezza del blocco nella coinbase, è un soft fork che è stato attivato il 15 novembre 2012.

Ha richiesto che l'altezza del blocco fosse inclusa nella transazione coinbase di ogni blocco.
Questo cambiamento ha migliorato la tracciabilità e ha reso più difficile la duplicazione di transazioni coinbase, rafforzando la sicurezza della rete.

BIP 322 Generic Signed Message Format

Livello: avanzato

Argomento: tecnologia

Il *Generic signmessage* è un metodo che consente ai wallet di firmare o parzialmente firmare un messaggio per qualsiasi script da cui si possa spendere.

Il BIP322 Generic Signed Message Format consente a un wallet di firmare una stringa di testo producendo una firma per una transazione virtuale di Bitcoin. Ciò significa che un messaggio firmato può essere prodotto per qualsiasi script o indirizzo che un wallet sarebbe in grado di spendere. Inoltre, due o più wallet possono collaborare per creare un messaggio firmato BIP322 per script multisig.

Il BIP322 definisce un formato standard per la firma di messaggi arbitrari con chiavi private Bitcoin. In sostanza, consente agli utenti di firmare messaggi arbitrari utilizzando le loro chiavi private Bitcoin e di fornire la prova della proprietà della chiave privata senza effettuare una transazione sulla blockchain.

I casi d'uso possono essere:

- semplice caso d'uso offline: firma utilizzando una chiave privata secp256k1 ECDSA or Schnorr
- semplice caso d'uso bitcoin: firma utilizzando un indirizzo bitcoin, sia una transazione di spesa che un UTXO
- semplice caso d'uso per identità (#w3c did:key?)
- caso d'uso complesso per l'identità (#w3c did:btcr2?)
- casi d'uso per varianti come P2WSH, P2TR, multisig, time lock, e PSBT

Può essere utile anche per esigenze di Travel Rule, Proof of Reserves, AML/KYC.

Quando si firma per gli indirizzi P2PKH legacy, BIP322 utilizza invece il formato di firma tradizionale "signmessage" che è stato implementato per la prima

volta in una versione precedente del software Bitcoin, rendendo la proposta retrocompatibile con il software esistente che verifica i messaggi firmati per gli indirizzi P2PKH.

BIP 324 (Version 2 P2P Encrypted Transport Protocol)

Livello: avanzato

Argomento: tecnologia

La BIP 324 (Version 2 P2P Encrypted Transport Protocol) è una proposta di miglioramento di Bitcoin che mira a migliorare la privacy dei nodi Bitcoin crittografando la loro comunicazione. Questa proposta introduce un nuovo protocollo di trasporto dei messaggi che crittografa e autentica i messaggi tra i nodi. Inoltre, costringe gli aggressori che ascoltano le comunicazioni tra i nodi a diventare attivi e rivelarsi.

La BIP-324 introduce un nuovo protocollo di trasporto P2P Bitcoin, che presenta crittografia opportunistica, una leggera riduzione della larghezza di banda e la possibilità di negoziare gli aggiornamenti prima dello scambio di messaggi applicativi.

Precedentemente i dati trasmessi nella rete P2P Bitcoin sono intrinsecamente pubblici e il protocollo non aveva una nozione di identità crittografiche, i peer comunicavano tra loro attraverso connessioni non crittografate e non autenticate. Tuttavia, questa natura in chiaro dell'attuale protocollo P2P (chiamato v1 in questo contesto) presenta gravi inconvenienti in presenza di attaccanti. La BIP 324 che introducendo una nuova versione del protocollo P2P (v2) mira a migliorare questo aspetto aumentando notevolmente i costi per eseguire questi attacchi, principalmente attraverso l'uso di crittografia di trasporto opportunistica non autenticata. Inoltre, il flusso di byte sul wire è reso pseudo-casuale (cioè indistinguibile da byte casuali uniformi) a un eavesdropper passivo.

Attualmente, i messaggi P2P di Bitcoin vengono trasmessi in testo chiaro, il che li rende vulnerabili all'intercettazione da parte di entità infrastrutturali come gli ISP, Internet Service Provider o fornitori di connessioni internet. Tali entità possono manomettere, eliminare o ritardare i messaggi tra peer anonimi. Un'entità infrastrutturale malintenzionata (o anche semplicemente costretta) potrebbe utilizzare questo per influenzare la topologia della rete, determinare l'origine delle transazioni o eseguire attacchi contro protocolli off-chain.

La BIP 324 crittografa i messaggi P2P utilizzando la codifica a flusso ChaCha20 con un codice di autenticazione dei messaggi Poly1305. Una sessione BIP 324 inizia con uno scambio di chiavi Diffie Hellman a curva ellittica per stabilire una chiave di sessione condivisa tra i peer. Da questa chiave di sessione condivisa, vengono derivate 2 chiavi, K_1 e K_2. K_1 viene utilizzato per crittografare la lunghezza del pacchetto di 3 byte. K_2 viene utilizzato per crittografare e autenticare il resto del pacchetto. Utilizzando le chiavi simmetriche K_1 e K_2, il ricevitore decripta prima il numero di lunghezza e da questo offset autentica il

pacchetto. Se l'autenticazione ha esito positivo, il ricevitore decripta il payload del messaggio e lo consegna allo strato di elaborazione.

La BIP 324 è stata implementata (merged) su Bitcoin Core a ottobre 2023.

Ecco alcuni dei vantaggi della BIP 324:

- Migliora la privacy degli utenti proteggendo i loro messaggi P2P dall'intercettazione.
- Rende più difficile per gli attaccanti manomettere o ritardare i messaggi P2P.
- Protegge la rete Bitcoin da attacchi che sfruttano la visibilità dei messaggi P2P.
- La BIP 324 è un passo importante verso una rete Bitcoin più sicura e privata.

Con il rilascio della versione Bitcoin Core 26.0 a dicembre 2023 viene incluso il supporto sperimentale a BIP324.

BIP 325 Signet

Livello: avanzato

Argomento: tecnologia

Signet (BIP 0325) è una nuova testnet, rete di test, per Bitcoin che aggiunge un ulteriore requisito di firma per la convalida dei blocchi.
Signet è simile a testnet, ma più affidabile e controllata centralmente. Esiste una rete di signet predefinita ("Signet Global Test Net VI"), ma chiunque può eseguire la propria signet a proprio piacimento.

A differenza della testnet, su Signet non ci sono miner. I blocchi vengono creati automaticamente dall'operatore di Signet ogni 10 minuti circa, senza bisogno della verifica Proof of Work.
Questo approccio rende lo sviluppo più prevedibile e simula in modo più accurato la mainnet.
Per questo motivo, la maggior parte degli sviluppatori preferisce testare su Signet invece che sulla testnet.

Signet è supportato di default da Bitcoin Core e dai nodi Bitcoin, e per attivarla è sufficiente modificare la configurazione per utilizzare Signet invece di mainnet.

BIP 340 (Schnorr Signatures)

Livello: avanzato

Argomento: tecnologia

BIP 340 introduce le firme Schnorr (Schnorr signatures) in Bitcoin Core. Le firme Schnorr offrono diversi vantaggi significativi rispetto a ECDSA, lo schema di firma digitale che Bitcoin ha utilizzato sin dall'inizio. In BIP 340 è inclusa

una descrizione dettagliata di come le firme Schnorr possono essere create e convalidate. Inoltre, vengono definiti nuovi formati per le firme Schnorr e le chiavi pubbliche. Le chiavi pubbliche Schnorr saranno di 32 byte e le firme Schnorr saranno lunghe 64 byte, rispetto alle chiavi e alle firme pubbliche ECDSA, che sono lunghe rispettivamente 33 e 70-72 byte. Questi piccoli risparmi di spazio consentono di risparmiare sulle commissioni di transazione per gli utenti Bitcoin che utilizzano Schnorr. Insieme a BIP 341 e BIP 342, BIP 340 è parte integrante dell'aggiornamento Taproot.

BIP 341 (Taproot)

Livello: avanzato

Argomento: tecnologia

BIP 341 definisce Pay-to-Taproot (P2TR), un nuovo modo di inviare bitcoin. P2TR combina le funzionalità degli script Pay-to-Public-Key (P2PK) e Pay-to-Script-Hash (P2SH), offrendo agli utenti grande flessibilità e vantaggi per la privacy. Mentre BIP 341 definisce P2TR, il nuovo tipo di output di Taproot, BIP 342 definisce Tapscript, un aggiornamento del linguaggio di scripting di Bitcoin che consentirà ai nodi Bitcoin di convalidare gli input Pay-to-Taproot. Taproot utilizzerà lo schema di firma Schnorr, come definito in BIP 340. Insieme, BIP 340, 341 e 342 comprendono l'aggiornamento Taproot.

BIP 342 (Tapscript)

Livello: avanzato

Argomento: tecnologia

BIP 342 definisce Tapscript, un aggiornamento del linguaggio di scripting di Bitcoin. Tapscript consente ai nodi Bitcoin di creare e convalidare gli output Pay-to-Taproot (P2TR) aggiornando gli opcode utilizzati da Bitcoin per valutare gli script.

Tapscript cambia il modo in cui le firme vengono valutate per sfruttare i miglioramenti di efficienza di Schnorr Signatures. Inoltre, BIP 342 aggiunge diversi nuovi opcode null, chiamati OP_SUCCESS, che consentono di aggiornare in modo flessibile Tapscript in futuro.

La proposta di miglioramento Bitcoin 342 fa parte dell'aggiornamento Taproot, che include anche BIP 340 e BIP 341.

BIP 38 (Passphrase-protected private key)

Livello: avanzato

Argomento: tecnologia

La BIP 38 ha permesso ai titolari di wallet di criptare le chiavi private di Bitcoin con una password per offrire un ulteriore livello di protezione.

Una chiave privata crittografata richiede che l'utente sia in possesso sia della chiave privata che della password per poter accedere ai fondi del wallet. Questo rende la gestione della chiave privata un passo di importanza critica, dove il BIP 38 è comunemente usato per i paper wallet e altri dispositivi analogici a scopo di sicurezza.

Proposto nel 2012, oggi molti wallet supportano questo metodo, che prevede l'utilizzo di una password per trasformare le chiavi criptate in chiavi decifrabili da un qualsiasi wallet.

La necessità d'uso di questo tipo di crittazione è dovuta al fatto che le chiavi sono stringhe lunghe di caratteri impossibili da ricordare, la necessità di scriverle su un paper wallet o inviarle e custodirle digitalmente le sottopone al rischio di essere intercettate con il rischio della perdita dei relativi fondi.

Se però la chiave è criptata, intercettando la comunicazione non si può sottrarre i fondi senza conoscere la password o passphrase. Per importare una chiave privata BIP38 su un qualsiasi wallet è necessario prima de-crittarla utilizzando la passhprase.

BIP 39 (Mnemonic Phrases)

Livello: avanzato

Argomento: tecnologia

BIP 39 è stato uno dei BIP bitcoin più importanti per migliorare il modo in cui le persone eseguono il backup delle proprie chiavi.

Il BIP39 definisce uno standard per la generazione di un "codice mnemonico" leggibile dall'uomo (noto anche come Seed Words) a partire da una fonte di entropia. Le Seed Words sono molto più facili da gestire per l'uomo rispetto alle lunghe stringhe di lettere e numeri definite nel BIP32. Grazie alla natura semplificata dei codici mnemonici, BIP39 è stato ampiamente adottato dal 99% dei wallet Bitcoin attualmente utilizzati.

Insieme a BIP 32 e BIP 44, costituisce le basi sulle quali vengono realizzati attualmente i wallet.

BIP 39 ha introdotto lo standard delle frasi mnemoniche. Le frasi mnemoniche offrono un metodo standardizzato per convertire un seed (seme) in una serie di 12-24 parole.
BIP-39 descrive l'implementazione di un codice mnemonico o di una frase mnemonica per la generazione di wallet HD (deterministici).
Consiste di due parti, che generano il mnemonico e lo convertono in un seed binario. Questo seed può quindi essere utilizzato in seguito per generare wallet HD utilizzando BIP-32 o metodi simili.

Quindi, una frase mnemonica dovrebbe essere tutto ciò che serve per recuperare tutte le chiavi private di un wallet.

La wordlist è creata in modo tale che sia sufficiente digitare le prime quattro lettere di ogni parola per identificarla univocamente. Le coppie di parole che sembrano simili vengono evitate per rendere molto più facile ricordare la frase. L'elenco di parole è ordinato in modo che la ricerca delle parole in codice sia più efficiente.
Per la conversione del mnemonico in seed, viene utilizzata la funzione PBKDF2.

BIP 44 (Derivation Paths for P2PKH)

Livello: avanzato

Argomento: tecnologia

BIP 44 definisce il Derivation Path standard per i wallet che generano indirizzi Pay-to-Public-Key-Hash (P2PKH).

BIP 44 definisce anche i prefissi da utilizzare con le chiavi estese associate.

Secondo BIP 44, i wallet che generano indirizzi P2PKH dovrebbero utilizzare un percorso di derivazione che inizia con "m/44'/"

Ciò significa che il primo indirizzo generato da un wallet Bitcoin mainnet avrà un percorso di derivazione:

`m/44'/0'/0'/0/0`

Inoltre, tutti questi wallet che utilizzano bitcoin mainnet dovrebbero utilizzare il prefisso "xpub" o "xprv" rispettivamente per le chiavi pubbliche e private estese.

Le chiavi estese che utilizzano lo standard BIP 44 sono quindi chiamate rispettivamente xpubs e xprvs. Se il wallet è un wallet testnet, vengono invece utilizzati i prefissi "tpub" e "tprv".

Questo standard è stato implementato per garantire che i wallet Hierarchical Deterministic (HD), come definito in BIP 32, possano importare chiavi estese e trovare il bitcoin memorizzato su quel wallet. Lo schema del wallet HD definisce un metodo per derivare un numero praticamente illimitato di chiavi pubbliche e private da un'unica chiave estesa.

Tuttavia, se una chiave estesa viene importata in un wallet senza alcuna guida, potrebbe essere difficile per il wallet trovare le chiavi con bitcoin, un requisito per visualizzare il saldo corretto per l'utente. Gli standard stabiliti da BIP 44, insieme a BIP 49 e BIP 84, risolvono questo problema. Quando un wallet importa una chiave estesa, il prefisso indica esattamente quale percorso di derivazione utilizzare per trovare bitcoin e derivare nuovi indirizzi.

Purtroppo anche i wallet che fanno riferimento al BIP44 possono aver interpretato l'implementazione in modo inconsistente.

In base al BIP44, questa gerarchia consiste di 5 livelli dopo la prima lettera separati dallo slash, con i seguenti significati:

m / purpose' / coin_type' / account' / change / address_index

BIP 47 (Reusable Payment Codes for HD Wallets)

Livello: avanzato

Argomento: tecnologia

Il BIP47 è un BIP Bitcoin Improvement Proposal o proposta di miglioramento bitcoin, per creare codici di pagamento riutilizzabili, proteggendo la privacy degli utenti per i pagamenti ricorrenti.
Senza il BIP47, gli utenti devono generare manualmente nuovi indirizzi per evitare l'Address reuse o la riutilizzazione di indirizzi.

Quando un utente riutilizza un indirizzo per le transazioni, consente a chiunque stia osservando la blockchain di raggruppare facilmente tutte le transazioni appartenenti all'indirizzo riutilizzato e formare un grafico della storia dei pagamenti dell'utente e del suo patrimonio.
Prevenire la riutilizzazione degli indirizzi è quindi una pratica migliore per la privacy in Bitcoin e già implementata in molte wallet Bitcoin per impostazione predefinita.
Tuttavia, quando un utente vuole stabilire pagamenti ricorrenti con un'altra parte, come in una relazione commerciante-cliente, la generazione frequente di nuovi indirizzi può essere scomoda.

Con il BIP47, un cliente può generare un set di indirizzi da utilizzare per i pagamenti per il commerciante. Se un cliente acquista prodotti mensilmente, il commerciante dovrebbe inviare al cliente un indirizzo ogni mese. Con il BIP47, il cliente crea un codice di pagamento dedicato per il commerciante, che funziona in modo simile a una chiave pubblica estesa.
Ciò consente al cliente di generare automaticamente nuovi indirizzi per il commerciante, invece che il commerciante dover creare indirizzi per il cliente.

Il BIP47 utilizza gli indirizzi di notifica, che sono monitorati dai wallet HD per gli output. In una transazione di notifica, il commerciante invia al cliente una blinded public key, una chiave pubblica offuscata, e un codice di catena tramite il campo OP_RETURN, insieme a un segreto condiviso per mantenere privati gli indirizzi condivisi sulla blockchain pubblica.
Questo scambio crea diversi problemi a causa dell'architettura della rete Bitcoin. I primi due sono economici: una transazione di notifica consiste in 80 byte, che possono diventare costosi per gli utenti quando le commissioni sulla rete Bitcoin sono alte. Le transazioni di notifica, inoltre, creano output non inviabili, che gonfiano l'UTXO Set nel tempo. Ciò aumenta il carico di calcolo sui nodi Bitcoin che, al momento, devono memorizzare l'intero UTXO Set, ovvero ogni output Bitcoin che non è stato utilizzato come nuovo input per garantire la validità delle transazioni.

BIP47 definisce lo standard per la creazione di un codice di pagamento che può essere pubblicizzato pubblicamente e associato a un'identità reale (o a uno pseudonimo) senza creare la perdita di sicurezza o di privacy insita nel riutilizzo degli indirizzi.

A differenza dei normali indirizzi Bitcoin, un codice di pagamento BIP47 viene utilizzato tra le parti coinvolte (mittente e destinatario) per generare un nuovo indirizzo ogni volta che viene effettuato un pagamento, evitando il riutilizzo degli indirizzi.

Il BIP47 non definisce un tipo di indirizzo, ma definisce un modo per un utente di generare indirizzi che possano essere usati da un altro utente senza dover interagire direttamente con lui e conoscendo solo il suo codice di pagamento pubblico.

Ecco un breve riassunto di come funziona. Nell'esempio, Alice paga Bob:

1. Alice riceve il codice di pagamento di Bob. Oltre ad alcuni metadati, questo codice contiene l'xpub di Bob al Derivation Path 47;

- Alice prepara una transazione di notifica. Sceglie uno dei suoi UTXO e crea un segreto condiviso S = k.B, dove k è la chiave privata di uno dei suoi UTXO e B è la prima chiave pubblica dell'xpub di Bob. Cifra il proprio codice di pagamento applicando lo XOR tra il proprio codice e HMAC-SHA512(o, Sx), dove o è il precedente punto di uscita dell'UTXO e Sx è la coordinata X di S;
- Invia la transazione all'indirizzo di notifica di Bob, che è il primo indirizzo dell'xpub di Bob, includendo il suo codice di pagamento criptato nell'OP_RETURN;
- Bob legge l'OP_RETURN e trova S = b.K, dove b è la chiave privata di B e K la chiave pubblica di k. Bob ottiene K e o dalla transazione di notifica. Con queste informazioni è in grado di recuperare il codice di pagamento di Alice;
- Alice può ora ricavare nuovi indirizzi e inviare pagamenti a Bob moltiplicando la chiave privata a dal suo codice di pagamento e le chiavi pubbliche B0, B1, B2 ecc. di Bob dal suo codice di pagamento.
  Bob farà il contrario: b0.A, b1.A, b2.A ecc;

BIP 48 (Multi-Script Hierarchy for Multi-Sig Wallets)

Livello: avanzato

Argomento: tecnologia

Il BIP48 definisce una gerarchia logica per i wallet multisig deterministici basata su un algoritmo descritto nel BIP67. Questo BIP consolida la pratica diffusa nel settore di utilizzare i percorsi di derivazione m/48' nei wallet multisig gerarchici deterministici. La gerarchia proposta consente la gestione di più account, la

ricezione e la modifica di elenchi di indirizzi per account, più tipi di script e milioni di indirizzi per chain.

Alcuni portafogli utilizzano lo schema di derivazione m/48' per gli account HD multi-sig. Questo BIP intende mantenere l'uso *esistente* nel mondo reale della derivazione m/48'. Non vengono apportate modifiche sostanziali per evitare "perdite di fondi" agli utenti esistenti. I portafogli che attualmente supportano la derivazione m/48' non dovranno apportare alcuna modifica per conformarsi a questa BIP.

BIP 49 (Derivation Paths for Wrapped Segwit)

Livello: avanzato

Argomento: tecnologia

BIP 49 definisce il derivation path standard per i wallet che generano indirizzi Wrapped SegWit (P2SH-P2WPKH).

BIP 49 definisce anche i prefissi da utilizzare con le chiavi estese associate. Secondo BIP 49, i wallet che generano indirizzi Wrapped SegWit dovrebbero utilizzare un derivation path che inizia con `m/49'/`

Ciò significa che il primo indirizzo generato da un wallet Bitcoin mainnet avrà un derivation path di `m/49'/0'/0'/0/0`

Inoltre, tutti questi wallet che utilizzano Bitcoin della mainnet dovrebbero utilizzare i prefissi ypub o yprv rispettivamente per le chiavi pubbliche e private estese. Le chiavi estese che seguono lo standard BIP 49 sono quindi chiamate rispettivamente **ypub** e **yprv**. Se il wallet è un wallet testnet, vengono invece utilizzati i prefissi **upub** e **uprv**.

Questo standard è stato implementato per garantire che i wallet HD, Hierarchical Deterministic, come definito in BIP 32, possano importare chiavi estese e trovare il bitcoin memorizzato su quel wallet.

Lo schema del wallet HD definisce un metodo per derivare un numero praticamente illimitato di chiavi pubbliche e private da un'unica chiave estesa. Tuttavia, se una chiave estesa viene importata in un wallet senza alcuna guida, potrebbe essere difficile per il wallet trovare le chiavi con bitcoin, un requisito per visualizzare il saldo corretto per l'utente.

Gli standard stabiliti da BIP 49, insieme a BIP 44 e BIP 84, risolvono questo problema. Quando un wallet importa una chiave estesa, il prefisso indica esattamente quale derivation path utilizzare per trovare bitcoin e derivare nuovi indirizzi.

BIP 68 nSequence

Livello: avanzato

Argomento: tecnologia

nSequence è un time lock relativo che opera a livello di transazione.

nSequence permette di specificare il tempo più precoce quando una transazione può essere aggiunta ad un blocco. Cioè, evitano la conferma di una transazione fino a quando una certa età è trascorsa negli output della transazione. Questa età può essere misurata in blocchi confermati o in tempo trascorso.

nSequences permette la creazione e la programmazione di più condizioni temporali sulla stessa transazione Bitcoin utilizzando lo script Bitcoin. Le quali, pur essendo diverse, saranno correlate l'una all'altra, quindi devono essere pienamente rispettate affinché la transazione possa essere convalidata e inclusa in un blocco della blockchain. Nel caso in cui tutte le condizioni stabilite non siano soddisfatte, la transazione semplicemente non può essere convalidata e fino ad allora sarà rifiutata dalla rete.

BIP 69 (Lexicographical Indexing of Transaction Inputs and Outputs)

Livello: avanzato

Argomento: tecnologia

Il BIP69 Lexicographical Indexing of Transaction Inputs and Outputs, Indicizzazione lessicografica degli input e degli output delle transazioni, è una proposta BIP di miglioramento del protocollo per la gestione dell'ordinamento degli input e degli output delle transazioni Bitcoin.

Il BIP-69 introduce un ordinamento "lessicografico" per gli input e gli output delle transazioni, in modo che le transazioni possano essere ordinate in modo deterministico.

Ciò significa che gli input e gli output delle transazioni vengono ordinati in base al loro valore in byte, invece di utilizzare un ordine casuale.

Ciò consente una maggiore prevedibilità e prevenzione degli errori nella creazione e nella gestione delle transazioni.

BIP 70 payment protocol

Livello: avanzato

Argomento: tecnologia

Il processo specifico per pagare utilizzando bitcoin si chiama Bitcoin Payment Protocol ed è codificato in un documento chiamato BIP70. Questo BIP descrive un protocollo per la comunicazione tra un commerciante e il suo cliente, consentendo sia una migliore esperienza del cliente che una migliore sicurezza contro gli attacchi man-in-the-middle (a volte abbreviato MITM) nel processo di pagamento. Nota che un attacco man-in-the-middle si verifica quando un cliente

si connette a un commerciante e si scopre che il cliente non sta realmente parlando con il commerciante, ma il cliente sta parlando con un uomo posizionato nel mezzo della comunicazione tra il cliente e il commerciante. Questo "uomo" può vedere tutto il traffico in corso tra il cliente e il venditore ed è quindi in grado di ottenere nomi utente, password e informazioni sulla carta di credito e tutto quel genere di cose personali, imitando il venditore. Con una buona imitazione il cliente probabilmente non sarà più saggio. Gli attacchi MITM sono insidiosi e le tecnologie (come il protocollo di pagamento BIP70) per prevenirli sono importanti.

BIP 8 (SFA)

Acronimo di: Soft Fork Activation

Livello: avanzato

Argomento: tecnologia

BIP 8 ha proposto un metodo alternativo al BIP 9 per l'attivazione dei soft fork. BIP 8 assomiglia molto a BIP 9, con alcune importanti modifiche, che hanno lo scopo di migliorare gli svantaggi percepiti di BIP 9.

Innanzitutto, BIP 8 utilizza l'altezza del blocco, anziché i timestamp per determinare l'ora di inizio e la durata del periodo di segnalazione. Questa piccola modifica ha un impatto relativamente limitato sul normale processo di attivazione, ma elimina la possibilità che un calo precipitoso del tasso di hash faccia deragliare l'attivazione di un aggiornamento.

In secondo luogo, BIP 8 implementa un flag opzionale che, se impostato a true, forza l'attivazione dell'upgrade anche se la soglia per il supporto del miner, solitamente 95%, non viene raggiunta prima della fine del periodo di segnalazione. BIP 8 utilizza la segnalazione della hash rate come metodo per accelerare l'attivazione per aggiornamenti estremamente popolari, piuttosto che come meccanismo per l'attivazione.

BIP 84 (Derivation Paths for Native Segwit)

Livello: avanzato

Argomento: tecnologia

Il BIP84 definisce lo standard per la derivazione degli indirizzi P2WPKH (Pay to Withness Public Key Hash), tipicamente indicati come indirizzi "Native Segwit". Gli indirizzi Segwit che iniziano con "bc1q" sono il tipo di indirizzo più comunemente utilizzato dai portafogli bitcoin moderni. Ciò è dovuto alla loro capacità di costruire transazioni più piccole che consentono all'utente di risparmiare sulle spese.

Il BIP84 definisce inoltre che i portafogli che adottano lo standard devono adottare i prefissi zpub o zprv quando visualizzano chiavi pubbliche/private

estese.

BIP 84 definisce il Derivation Path standard per i wallet che generano indirizzi SegWit (P2WPKH) nativi. BIP 84 definisce anche i prefissi da utilizzare con le chiavi estese associate.

Secondo BIP 84, i wallet che generano indirizzi SegWit nativi dovrebbero utilizzare un derivation path che inizia con m/84'/ Ciò significa che il primo indirizzo generato da un wallet Bitcoin mainnet avrà un derivation path di m/84'/0'/0'/0/0

Inoltre, BIP 84 afferma che tutti i wallet che utilizzano SegWit nativo su mainnet dovrebbero utilizzare i prefissi zpub o zprv rispettivamente per le chiavi pubbliche e private estese. Le chiavi estese che seguono lo standard BIP 84 sono quindi chiamate rispettivamente zpubs e zprvs. Se il wallet è del tipo testnet, vengono utilizzati i prefissi vpub e vprv

Questo standard è stato implementato per garantire che i wallet Hierarchical Deterministic (HD), come definito in BIP 32, possano importare chiavi estese e trovare il bitcoin memorizzato su quel wallet.

Lo schema del wallet HD definisce un metodo per derivare un numero praticamente illimitato di chiavi pubbliche e private da un'unica chiave estesa. Tuttavia, se una chiave estesa viene importata in un wallet senza alcuna guida, potrebbe essere difficile per il wallet trovare le chiavi con bitcoin, un requisito per visualizzare il saldo corretto per l'utente.

Gli standard stabiliti da BIP 84, insieme a BIP 44 e BIP 49, risolvono questo problema. Quando un wallet importa una chiave estesa, il prefisso indica esattamente quale derivation path utilizzare per trovare bitcoin e derivare nuovi indirizzi

BIP 85 (Deterministic Entropy From BIP32 Keychains)

Livello: avanzato

Argomento: tecnologia

Il BIP-85 offre una soluzione alla sfida di avere troppe recovery phrase segrete e di doverne eseguire il backup in modo sicuro. Definisce un modo per derivare nuove recovery phrase segrete da una recovery phrase segreta principale. Il vantaggio è che si dispone di una recovery phrase segreta di cui si esegue il backup e da cui si generano nuove recovery phrase segrete multiple (per wallet diversi). Senza BIP85, ci si potrebbe ritrovare con decine di recovery phrase segrete diverse di cui è necessario eseguire il backup.

Non è possibile mantenere un unico backup del seed (mnemonico) per tutte le keychain utilizzate nei vari wallet, poiché esistono diversi standard incompatibili. La condivisione dei seed tra diversi wallet non è auspicabile per motivi di

sicurezza. L'archiviazione fisica di più seed è difficile a seconda della sicurezza e della ridondanza richieste.

Poiché i wallet HD sono essenzialmente derivati dall'entropia iniziale, questa proposta fornisce un modo per ricavare l'entropia dal wallet che può essere inserita in qualsiasi metodo utilizzato da un wallet per ricavare il seed mnemonico iniziale o la chiave principale.

BIP 86 (Key Derivation for Single Key P2TR Outputs)

Livello: avanzato

Argomento: tecnologia

BIP86 è il BIP che definisce lo standard di derivazione per i wallet HD le cui chiavi sono coinvolte in uscite P2TR (Pay to Taproot) a chiave singola. Questi indirizzi Taproot iniziano con **bc1p** e non devono essere confusi con gli indirizzi "Native Segwit", dall'aspetto simile, che iniziano con "bc1q" e sono definiti nel BIP84.

Con l'uso di transazioni P2TR a chiave singola, è utile avere uno schema di derivazione comune in modo che i wallet HD che hanno solo un backup del seed HD possano recuperare i risultati Taproot a chiave singola. Sebbene oggi esistano soluzioni che ovviano alla necessità di Derivation Path fissi per specifici tipi di script, molti wallet software e hardware utilizzano ancora backup di seed che mancano di informazioni sul percorso di derivazione e sullo script. Per questo motivo, per facilitare l'implementazione, viene utilizzato lo stesso approccio utilizzato nei PIF 49 e 84.

BIP 9 (SFA)

Acronimo di: Soft Fork Activation

Livello: avanzato

Argomento: tecnologia

BIP 9 ha stabilito un framework standard per l'attivazione degli aggiornamenti soft fork al protocollo Bitcoin. Altri metodi per l'attivazione di soft fork, come BIP 8 e Modern Soft Fork Activation, sono derivati da BIP 9 con l'obiettivo di migliorare gli svantaggi percepiti di BIP 9.

Poiché l'attivazione dell'aggiornamento è un processo di consenso, BIP 9 descrive principalmente le decisioni e le azioni che dovrebbero essere intraprese dalla comunità, piuttosto che proporre modifiche al modo in cui funziona Bitcoin. BIP 9 definisce il seguente processo per l'attivazione di un soft fork.

Innanzitutto, il campo della versione nei blocchi Bitcoin viene riproposto come meccanismo di segnalazione per il supporto per gli aggiornamenti. Il campo

della versione è lungo 4 byte, quindi contiene 32 bit. Un singolo bit viene scelto come bit per questo aggiornamento.

In secondo luogo, la comunità deve decidere l'ora di inizio e la durata del periodo di segnalazione. Durante questo periodo, i miner segnaleranno il loro supporto per l'aggiornamento impostando il bit scelto su 0 o 1 in tutti i blocchi che minano.

Esaminando il bit scelto di ogni blocco minato durante il periodo di segnalazione, possiamo calcolare la percentuale di miner che supportano l'aggiornamento, ponderata per hash rate. Se, durante il periodo di segnalazione, il 95% dei blocchi segnala il supporto per l'aggiornamento, l'aggiornamento sarà considerato "locked in". A quel punto, l'aggiornamento verrà attivato dopo un breve periodo di tempo. Questo ritardo ha lo scopo di dare ad altri nodi e miner il tempo di adottare l'aggiornamento e prepararsi per eventuali nuove funzionalità.

Fatto chiave: poiché BIP 9 viene utilizzato per l'attivazione del soft fork e i soft fork sono per definizione compatibili con le versioni precedenti, i nodi e i miner non sono mai costretti ad eseguire l'aggiornamento.

Se la soglia del 95% per il supporto dei miner non viene raggiunta durante il periodo di segnalazione, l'attivazione dell'aggiornamento non riesce. Pertanto, BIP 9 mette la maggior parte del controllo sull'attivazione dell'aggiornamento nelle mani dei miner. BIP 8 e altri metodi di aggiornamento sono stati creati per dare ai nodi un maggiore controllo sull'attivazione dell'aggiornamento.

BIP352 silent payments

Livello: avanzato

Argomento: tecnologia

Il BIP352, noto anche come Silent Payments, è una proposta di miglioramento del protocollo Bitcoin firmata da Ruben Somsen e dallo sviluppatore josibake. Questa proposta mira a migliorare la privacy e l'anonimato delle transazioni Bitcoin, risolvendo alcune delle limitazioni esistenti nel sistema attuale.

In parole semplici, il BIP352 consente di inviare pagamenti Bitcoin senza rivelare l'indirizzo del destinatario o l'importo inviato. Questo è possibile attraverso un meccanismo che permette al mittente di creare un indirizzo temporaneo unico per ogni transazione, che può essere derivato da un'informazione pubblica condivisa dal destinatario. In questo modo, l'osservatore esterno non può facilmente correlare gli indirizzi di ricezione con l'identità del destinatario, aumentando significativamente la privacy.

Gli aspetti caratterizzanti del BIP352 includono:

- **Indirizzi Temporanei Unici**: Ogni pagamento utilizza un indirizzo unico che viene generato per la specifica transazione. Questo rende difficile per un osservatore esterno tracciare le transazioni verso uno specifico

indirizzo.

- **Privacy Migliorata**: Poiché gli indirizzi sono unici e temporanei, è molto più difficile per terze parti collegare diverse transazioni a uno stesso destinatario, migliorando così la privacy degli utenti.
- **Mantenimento della Compatibilità**: La proposta è progettata per essere compatibile con le infrastrutture esistenti di Bitcoin, il che significa che può essere adottata senza la necessità di cambiamenti radicali nel protocollo di base o nei software di wallet.
- **Facilità di Implementazione**: Il meccanismo proposto è relativamente semplice da implementare rispetto ad altre soluzioni di privacy avanzata, rendendo più probabile la sua adozione da parte della comunità Bitcoin.

Nel 2023, il BIP352 è stato formalizzato, segnando un passo importante verso la sua possibile integrazione nel protocollo Bitcoin. La formalizzazione indica che la proposta è stata adeguatamente discussa, documentata e accettata come un miglioramento potenziale per la rete Bitcoin.

Il BIP352 rappresenta un'importante evoluzione nel campo della privacy delle criptovalute, offrendo un livello di anonimato maggiore e proteggendo meglio gli utenti da analisi delle transazioni e da sorveglianza.

bit

Livello: intermedio

Argomento: tecnologia

Il termine bit in informatica viene utilizzato per indicare l'unità di informazione digitale che può valere 0 o 1.

Nei Bitcoin, questo termine viene utilizzato per indicare un'unità o subunità di un bitcoin, il milionesimo di Bitcoin. 1 milione di bit equivalgono a 1 bitcoin (BTC).

Tale unità è meno utilizzata rispetto al sat, il cui rapporto è 1 a 100, ovvero ci vogliono 100 sat per fare 1 bit.

Il termine bit non è più usato spesso per descrivere frazioni di bitcoin, ma c'è chi ne consiglia l'utilizzo e incoraggia di utilizzarlo perché utilizzare i Sat per indicare una frazione più piccola di Bitcoin può creare confusione per l'utente medio.

Tra questi Adam Back, l'unica persona citata nel white paper Bitcoin, secondo il quale
"*Apparentemente, i primi bitcoin avevano solo BTC e vecchi bitcents. 2,1 miliardi di vecchi bitcents corrispondevano a 21 milioni di BTC.*
La storia che ho sentito dai primi sviluppatori è che Hal Finley ha convinto Satoshi che non fosse sufficiente per la popolazione mondiale, quindi Satoshi ha aggiunto 1 milione di suddivisioni, spostando il nuovo bitcent a 1/100 di bit, con un bit che rappresentava la milionesima parte di un bitcoin. Dove 1 bit = 100

bitcents, come ad esempio 3,45 bit = 3 bit e 45 bitcents.
Successivamente, la comunità ha affettuosamente chiamato il bitcent Satoshi o sat per abbreviare. Ma a quanto pare, era destinato a essere un bitcent decimale a due cifre dopo l'unità di base più piccola, il bit."

Bit Gold

Livello: avanzato

Argomento: economia

Nick Szabo cercò di lanciare BitGold, una valuta digitale decentralizzata in cui per la prima volta si poneva l'accento sulla distribuzione comunitaria della gestione della valuta e sulla creazione di un algoritmo Proof of Work per limitarne la produzione ed evitare fenomeni inflazionistici.

Szabo non ebbe però fortuna nell'attrarre attenzione sulla sua creazione.

Bit Gold, ideato da Nick Szabo nel 1998 (ma pubblicato più ampiamente nel 2005), è considerato uno dei precursori più importanti e diretti di Bitcoin. Condivide diverse somiglianze con Bitcoin e ha introdotto concetti fondamentali che sono stati poi ripresi e raffinati nella creazione della prima criptovaluta di successo.

Ecco i punti chiave di Bit Gold:

1. Scarsità Digitale e Proof-of-Work:

- Problema da risolvere: Bit Gold mirava a creare un bene digitale scarso e indipendente da un'autorità centrale, simile all'oro.
- Soluzione: Szabo propose di utilizzare catene di funzioni hash computazionalmente costose (Proof-of-Work) come soluzione. I partecipanti avrebbero dovuto risolvere complessi problemi crittografici, e la soluzione (una stringa di bit) sarebbe diventata "bit gold".
- Collegamento all'oro: La difficoltà di estrazione dell'oro, che ne limita l'offerta e ne preserva il valore, era il modello di riferimento. Il Proof-of-Work di Bit Gold replicava questa difficoltà computazionalmente.
- Timestamping: Le soluzioni di Proof-of-Work sarebbero state timestampate (registrate con una marca temporale) e pubblicate in un registro distribuito.

2. Architettura Distribuita:

- Registro Pubblico: Bit Gold prevedeva un sistema di registri distribuiti (titoli di proprietà) dove le soluzioni di Proof-of-Work, e le successive transazioni, sarebbero state registrate pubblicamente.
- Database Replicati: Questo registro sarebbe stato replicato e mantenuto da un network di partecipanti, non da un'autorità centrale.

- Sicurezza e consenso: La sicurezza del sistema si basava sulla maggioranza onesta dei partecipanti (in termini di potenza di calcolo) che avrebbero validato le transazioni e mantenuto l'integrità del registro.

3. Transazioni e Proprietà:

- Trasferimento di Proprietà: La proprietà del "bit gold" (le stringhe di bit derivate dal Proof-of-Work) poteva essere trasferita collegando crittograficamente la chiave pubblica del nuovo proprietario alla stringa di bit gold.
- Firme Digitali: Le transazioni sarebbero state firmate digitalmente per garantirne l'autenticità.

4. Sfide e Limiti di Bit Gold: Nonostante le sue innovative caratteristiche, Bit Gold presentava alcune sfide che ne hanno impedito l'implementazione pratica:

- Problema della Doppia Spesa (Parzialmente Risolto): Szabo propose un sistema basato su un quorum di server per prevenire la doppia spesa, ma non era una soluzione completamente decentralizzata e immune agli attacchi Sybil (dove un attaccante crea molteplici identità fittizie per ottenere il controllo del network).
- Inflazione: Anche se il Proof-of-Work rendeva la creazione di "bit gold" costosa, non c'era un meccanismo chiaro per limitare l'offerta a lungo termine, il che avrebbe potuto portare a un'inflazione.
- Complessità e Scalabilità: Il sistema, per come era stato concepito, era complesso e poneva dubbi sulla sua scalabilità per gestire un elevato volume di transazioni.

5. Eredità e Influenza su Bitcoin: Nonostante le sue lacune, Bit Gold è stato un precursore fondamentale di Bitcoin. Ha introdotto e combinato concetti chiave come:

- Scarsità digitale basata sul Proof-of-Work.
- Registro pubblico distribuito per le transazioni.
- Uso di firme digitali per l'autenticazione delle transazioni. Satoshi Nakamoto, il creatore di Bitcoin, ha riconosciuto l'influenza di b-money e Hashcash, ma non ha menzionato direttamente Bit Gold. Tuttavia, le somiglianze sono evidenti, e molti ritengono che Bitcoin abbia risolto i problemi di Bit Gold, in particolare quello della doppia spesa, attraverso l'invenzione della blockchain.
  s In conclusione, Bit Gold è un progetto di notevole importanza storica nel campo delle criptovalute. Pur non essendo mai stato implementato, ha contribuito in modo significativo a plasmare le idee che hanno portato alla nascita di Bitcoin, gettando le basi per la rivoluzione della moneta digitale.

Bitcoin

Livello: base

Argomento: tecnologia

Bitcoin è la prima criptovaluta, una forma di denaro digitale, creata da Satoshi Nakamoto che ne ha pubblicato a ottobre 2008 il white paper, e a gennaio 2009 il primo blocco della sua block chain, il Genesis block.

Bitcoin è una proprietà digitale che non può essere sequestrata, contraffatta o copiata.

Bitcoin trae valore dalle sue proprietà uniche: è resistente alla censura, permettendo agli individui nei regimi oppressivi di conservare e trasferire ricchezza senza interferenze statali. È senza confini, permettendo a miliardi di individui di partecipare all'economia globale. È senza permessi, il che significa che nessuna autorità centrale può controllarne l'accesso.

Bitcoin è un sistema monetario immutabile e decentralizzato con una fornitura fissa di 21 milioni di monete. La sua scarsità non è un espediente di marketing ma un principio economico—uno che rispecchia la fornitura limitata di oro, che ha servito come denaro per millenni.

Nessun governo, nessuna banca centrale, nessun burocrate ne detta il valore, che è determinato dal libero mercato, la massima espressione di valore.

La parola Bitcoin ha acquisito molteplici significati, pertanto li distinguiamo utilizzando termini più specifici.

Il termine Bitcoin viene usato come termine generico per racchiudere l'intero sistema, che può includere più livelli (compresi alcuni futuri) e l'idea generale del sistema di moneta elettronica peer-to-peer originato da Satoshi Nakamoto.

Allo stesso tempo, utilizziamo BTC per denotare Bitcoin come forma di scarsità digitale, denaro e valuta.

Distinguiamo anche il consenso Bitcoin PoW (la regola per selezionare il produttore del blocco successivo), il consenso Nakamoto (che include il consenso PoW migliorato con mezzi cripto-economici per punire i minatori), la block chain Bitcoin come implementazione specifica attuale del livello 1 di Bitcoin e il protocollo Bitcoin (BP) come insieme di standard, tecnologie e strumenti per lavorare con transazioni Bitcoin on-chain (in qualsiasi possibile livello 1).

Bitcoin viene classificato in molti modi, spesso in funzione di chi da la definizione e certi termini definiscono più chi le usa che Bitcoin stesso, perché Bitcoin è qualcosa di più di queste singole definizioni:

- Protocollo: Bitcoin è principalmente un protocollo: è un insieme di regole che definiscono come la criptovaluta funziona, e chiunque rispetti il protocollo può partecipare al network Bitcoin
- Hard money: Bitcoin non viene considerato una generica forma di denaro, ma Hard money ovvero una forma di denaro che è scarsa, limitata nella quantità e difficile da produrre

- Store of value, riserva di valore o bene rifugio: storicamente l'oro viene considerato lo store of value per eccellenza, e sempre più spesso Bitcoin viene definito come oro digitale
- Mezzo di scambio, o moneta merce, in inglese Medium of Exchange: per alcuni Bitcoin non avrebbe ancora le caratteristiche per essere considerato un mezzo di scambio, per altri si tratta solo di tempo perché lo diventi, e per altri ha già le proprietà per essere considerato uno dei migliori mezzi di scambio
- Commodity: l'agenzia americana SEC ha definito Bitcoin come commodity, in contrasto alle altre criptovalute che sono considerate security
- Cripto-attività: con questo termine, usato anche nel Testo Unico delle Imposte Dirette, si vuole evidenziare il ruolo di asset speculativo, quasi che serva solo per essere comprato e rivenduto a prezzo più alto con il solo scopo di guadagnare valute fiat; nonostante molti vedano esclusivamente questo aspetto, in realtà dovrebbe essere l'aspetto meno importante ed è probabile che nel lungo termine perda importanza l'uso di bitcoin come attività a vantaggio di altre proprietà come store of value e mezzo di scambio
- Crypto asset: il termine crypto asset è l'equivalente inglese di, ed è utilizzato tra l'altro dal MiCA il regolamento Europeo sui mercati nelle criptovalute, per definire Bitcoin
- Cryptocurrency o Criptovaluta, un tipo di valuta digitale protetta dalla crittografia
- Crypto: il termine crypto o in italiano critpo, sarebbe l'abbreviazione di cryptocurrency o criptovaluta, ma recentemente c'è la tendenza per alcuni bitcoiner a non utilizzare questo termine per bitcoin, per differenziarsi dalle altre criptovalute che vengono considerate shitcoin da alcuni massimalisti
- Valuta o Currency: Bitcoin potrebbe essere considerata una forma moderna di valuta
- Scarsità digitale

Bitcoin Core

Livello: base

Argomento: tecnologia

Bitcoin Core viene considerato l'implementazione che attualmente rappresenta lo standard de facto per Bitcoin.

Inizialmente il client era stato chiamato semplicemente Bitcoin o Bitcoin-QT, ma il nome Bitcoin Core venne adottato nel febbraio 2013.

Bitcoin Core è l'implementazione di riferimento per il codice sorgente di Bitcoin, il che significa che tutte le altre implementazioni guardano a Bitcoin Core per avere indicazioni sul mantenimento del consenso e sull'aggiornamento.

Bitcoin Core fornisce il software per un nodo e un wallet, anche se la maggior parte degli utenti preferisce usare Bitcoin Core per il nodo e utilizzare software di terze parti per il wallet. Esistono alternative al software del nodo di Bitcoin Core, ma Core è l'implementazione dominante.

Chiunque desideri scaricare il software di Bitcoin ed eseguire un nodo può accedere a Bitcoin Core tramite il suo sito web bitcoincore.org o la sua pagina GitHub github.com/bitcoin/bitcoin. È qui che la maggior parte degli utenti si reca per scaricare il codice sorgente.

Inizialmente il sito considerato di riferimento era bitcoin.org, che fu originariamente registrato da Satoshi Nakamoto e Martti Malmi, uno dei primi programmatori di Bitcoin. Quando Nakamoto lasciò il progetto, estese la proprietà del dominio ad altre persone. Il sito veniva utilizzato principalmente per il rilascio di nuove versioni del software. Nel 2013, il sito è stato ridisegnato e non può più essere considerato il sito ufficiale di Bitcoin.
Nel 2021, il sito bitcoin.org ha dovuto inibire agli utenti britannici l'accesso al whitepaper a causa di una causa intentata da Craig Wright, salvo poi ripristinarlo nel 2024, dopo che un tribunale ha stabilito che Craig Wright non è Satoshi Nakamoto.

Eseguendo il codice di Bitcoin Core, un utente agisce come un nodo della rete che può verificare in modo indipendente sia la validità della creazione dei blocchi sulla rete sia le transazioni inviate dagli utenti della rete.

Bitcoin Core è stato inizialmente creato da Satoshi Nakamoto, ma non è di proprietà di una singola entità, azienda o organizzazione. Viene aggiornato, mantenuto e revisionato da una comunità globale di sviluppatori e sebbene molti aggiornamenti siano stati aggiunti al progetto, l'ultima versione e quella originale di Satoshi sono ancora compatibili.

Bitcoin Core è un progetto open source. Ciò significa che chiunque può copiare il codice sorgente e modificarlo come meglio crede. Se uno sviluppatore vuole migliorare Bitcoin, può pubblicare le modifiche apportate e proporre di includerle nel Bitcoin Core. Molti sviluppatori scelgono di contribuire a Bitcoin Core attraverso il codice, la revisione e la discussione. Tuttavia, non esiste un'entità autorevole che paghi gli sviluppatori per lavorare a Bitcoin Core. Invece, le aziende e i privati finanziano parzialmente questi sviluppatori attraverso donazioni e sovvenzioni.

Il primo software per l'utilizzo di Bitcoin, scritto in linguaggio C++ e rilasciato da Satoshi Nakamoto nel 2009 col nome Bitcoin, includeva sia la funzione di wallet, che quella di nodo e anche quella di miner e può essere considerato la prima versione di Bitcoin Core, anche se il termine Core ancora non veniva utilizzato, con versione 0.1.0 disponibile solo per Windows. Con la successiva, la 0.2.0, è stato introdotto per la prima volta il supporto per i sistemi Linux e successivamente per MacOS.

Dalla versione 0.5.0 del 2011, il client con l'interfaccia grafica ha iniziato a

chiamarsi Bitcoin-QT.
Nel 2016 viene definitivamente rimossa la funzione di mining, e nella versione 0.9.0 viene reintrodotto il nome Bitcoin Core.
La necessità di rinominare il client deriva dal fatto che con Bitcoin si intende oggi la rete intera, composta da numerosi diversi client, scritti in linguaggi di programmazione differenti, i quali tuttavia seguono un protocollo comune che assicura la corretta interazione fra tutti i nodi della rete. Le repository considerate "ufficiali" di Bitcoin Core sono mantenute dal team "Core" sulla piattaforma github.

Sono anche stati resi disponibili nel tempo dei client per implementare un full node, quali

- Bitcoin Knots
- Libbitcoin
- nix-bitcoin
- btcd

Su btcd ad esempio è implementato la più diffusa versione del nodo Lightning Network: LND.

Chiunque è libero di creare un progetto alternativo, creando un nuovo branch su github a partire dal codice di Bitcoin Core, che se non rispettano il protocollo possono generare dei fork incompatibili.

Bitcoin dominance

Livello: intermedio

Argomento: finanza

La bitcoin dominance è un indicatore che misura la quota di mercato di Bitcoin rispetto ad altre criptovalute. Viene calcolata come il rapporto tra la capitalizzazione di mercato Bitcoin rispetto al valore totale di tutte le altre criptovalute in circolazione.

Purtroppo questo indicatore è fallace, perché è difficile avere dati affidabili sulle numerosissime criprovalute, vengono create continuamente nuove criptovalute e nuovi token, e queste comportano delle distorsioni. La fonte utilizzata per poter valutare le varie criptovaalute è il sito coinmarketcap, che può essere soggetto a distorsioni. Lo stesso concetto di capitalizzazione viene spesso criticato in quanto inadatto a rappresentare il valore di una criptovaluta.

La bitcoin dominance viene spesso utilizzata come un modo per valutare l'importanza di Bitcoin nel mercato delle criptovalute. Una bitcoin dominance elevata indica che il prezzo di Bitcoin è relativamente stabile e che il suo valore è dominante rispetto ad altre criptovalute. Una bitcoin dominance bassa, d'altro canto, potrebbe indicare che il mercato delle criptovalute è più volatile e che altre criptovalute stanno guadagnando terreno rispetto a Bitcoin.

È importante notare che la bitcoin dominance può variare notevolmente nel tempo a causa della volatilità del mercato delle criptovalute. Ad esempio, nel 2017, la bitcoin dominance era superiore al 90%, mentre nel 2021 è scesa al 50%.

BitDNS

Livello: avanzato

Argomento: tecnologia

BitDNS è un progetto che ha avuto come obiettivo quello di estendere la tecnologia di Bitcoin a un servizio DNS, per la gestione dei nomi a dominio, espandendo il software per supportare le transazioni per la registrazione, l'aggiornamento e il trasferimento dei domini. Il progetto è poi diventato un altcoin con il suo proprio altcoin, noto come Namecoin.

Nel settembre 2010 è iniziata una discussione sul forum di BitcoinTalk riguardo a un ipotetico sistema chiamato BitDNS.

Gavin Andresen e Satoshi Nakamoto hanno partecipato alla discussione sul forum di BitcoinTalk e hanno supportato l'idea di BitDNS, e nel dicembre 2010 fu stata annunciata sul forum una ricompensa per l'implementazione di BitDNS.

Con l'aggiornamento di mining merged attivato nel blocco 19200, Namecoin ha permesso la mining simultanea di Bitcoin e Namecoin, invece di dover scegliere tra uno o l'altro; ciò ha risolto il problema dei minatori che passavano da una blockchain all'altra quando la redditività diventava favorevole nel primo. Tuttavia, Satoshi respinse poi questa idea affermando che la combinazione di tutti i sistemi di consensus proof-of-work in un unico dataset non sarebbe stato scalabile. Come risultato, BitDNS è stato abbandonato e si è evoluto in una chain separata nota come Namecoin.

bLIP

Acronimo di: Bitcoin Lightning Improvement Proposal

Livello: avanzato

Argomento: tecnologia

bLIP è l'acronimo di Bitcoin Lightning Improvement Proposal. Un bLIP è un documento di progettazione che fornisce informazioni alla comunità Lightning Network o descrive una nuova funzionalità per Lightning Network.

Il bLIP deve fornire una specifica tecnica concisa della funzionalità e una motivazione per la stessa. L'autore del bLIP è responsabile della creazione del consenso all'interno della comunità e della documentazione delle opinioni dissenzienti. È importante sottolineare che se una caratteristica è destinata a diventare universale o quasi, deve essere un BOLT.

Chi desidera presentare delle bLIP deve prima proporre la propria idea alla mailing list di sviluppo di Lightning. Dopo la discussione, dovrebbe aprire una PR, una Pull Request.

Dopo il copy-editing e l'accettazione, la proposta viene pubblicata nella lista dei bLIP su github.

Block

Blocco

Livello: base

Argomento: tecnologia

Il blocco è un insieme di transazioni raggruppate dai miner e inserite nella block chain.

I miner raccolgono le transazioni in attesa di essere confermate dallo spazio transitorio chiamato mempool, selezionano le transazioni confezionando un block template che viene firmato in base all'algoritmo di consenso e trasmettono tale blocco alla rete dei nodi Bitcoin in modo che diventi parte della block chain.

Se pensiamo alla block chain come ad un Libro Mastro o Ledger, il blocco può essere considerato una pagina di questo libro.

Il blocco è costituito da due componenti principali:

- un Block Header
- le transazioni del blocco

Il blocco è identificato da un hash, calcolato sul Block Header.

Il primo blocco della block chain è chiamato Genesis block.

I blocchi della block chain Bitcoin sono stati nei primi anni limitati ad 1 MB di dati.

Con l'introduzione di SegWit è stata sostituita la Block size, o dimensione del blocco, da 1 MB con la Block Weight, che ha consentito di avere 4 milioni di weight unit in un blocco.

Nel 2015 è stato minato il blocco 367853 che contiene 12.239 transazioni.

Block Explorer

Livello: base

Argomento: tecnologia

La blockchain di Bitcoin è un registro pubblico di ogni transazione avvenuta. I block explorer forniscono una vista di questa storia.

Un block explorer (esploratore di blocchi) Bitcoin è un'applicazione o un servizio online che consente agli utenti di esaminare e tracciare le transazioni sulla blockchain di Bitcoin. La blockchain di Bitcoin è un registro pubblico decentralizzato che contiene tutte le transazioni effettuate con la criptovaluta. Ogni blocco nella blockchain contiene un elenco di transazioni e un riferimento al blocco precedente, creando così una catena di blocchi.

Un block explorer offre agli utenti la possibilità di cercare, visualizzare e analizzare le transazioni, i blocchi e gli indirizzi Bitcoin. Alcune delle informazioni fornite includono:

- Transazioni: Dettagli sulle transazioni, come gli indirizzi mittente e destinatario, l'importo trasferito e la tassa di transazione.
- Blocchi: Informazioni sui blocchi, come l'altezza del blocco, il timestamp di creazione e l'hash del blocco.
- Indirizzi: Dettagli sugli indirizzi Bitcoin, mostrando il saldo corrente e la cronologia delle transazioni associate.
- fee di transazione: Statistiche sulle commissioni di transazione, la dimensione media dei blocchi e altri dati relativi al funzionamento della rete.
- Stato della rete: Informazioni sulla salute e le statistiche generali della rete Bitcoin.

I block explorer sono strumenti utili per verificare la validità di una transazione, monitorare il progresso di una transazione in attesa di conferma, esplorare la cronologia delle transazioni di un indirizzo o ottenere informazioni sull'andamento generale della rete Bitcoin.

Alcuni dei block explorer più noti per Bitcoin includono mempool.space, Blockchair, Blockchain.com, e Blockstream Explorer.

Block header

Livello: avanzato

Argomento: tecnologia

La blockchain è costituita da una serie di blocchi che vengono utilizzati per memorizzare le informazioni relative alle transazioni che avvengono su una rete di blockchain. Ciascuno dei blocchi contiene un block header, un'intestazione unica e ogni blocco è identificato individualmente dall'hash del Block Header.

CONCETTI CHIAVE

- I block header identificano i singoli blocchi di una blockchain.
- Vengono sottoposti a hash nella proof of work.
- I blocchi sono stratificati verticalmente, a partire dal "blocco genesi".
- Ogni block header ha tre serie di metadati del blocco e più componenti individuali.
- Il numero di versione di Bitcoin aiuta a tenere traccia delle modifiche apportate al protocollo.

Il Block Header è quella parte di un blocco che serve a descrivere il resto del blocco, è grande 40 byte e contiene i seguenti campi:

Dimensione	Campo	Descrizione
4	version	Indica la versione del protocollo utilizzata per il blocco.
32	hash	L'hash del blocco precedente che permette di creare la catena di blocchi.
32	merkle root	La Merkle root delle transazioni incluse nel blocco.
4	timestamp	L'oradi creazione del blocco impostata dal miner
4	difficoltà	La difficoltà con la quale il blocco è stato minato
4	nonce	Un valore variabile usato dai miner per risolvere il puzzle di proof-of-work.

La dimensione è indicata in Byte.

In sostanza, il Block Header contiene i dati che definiscono il blocco, escluso l'elenco delle transazioni.

I miner calcolano l'hash del Block Header nella loro attività di mining di un blocco valido. Questo è molto più efficiente dell'hashing dell'intero blocco, che può essere composto da migliaia di transazioni. Sarebbe molto più complicato per un miner cambiare il nonce e rieseguire un intero blocco di 2 MB per ogni tentativo. Si confronti con l'hashing del block header di Bitcoin, ad esempio, che hanno una lunghezza fissa di 80 byte. I block header sono ottime dal punto di vista del mining, ma grazie alle loro dimensioni ridotte sono ideali anche per i light client. La blockchain di Bitcoin è troppo grande per essere memorizzata da dispositivi come gli smartphone. Se la catena avesse 100.000 blocchi da 1MB, si consumerebbero 100GB di spazio. Ma con le sole intestazioni degli stessi blocchi, si occuperebbero solo 0,008GB, ovvero 8MB. In questo modo, i dispositivi con meno larghezza di banda o spazio di archiviazione possono comunque eseguire un certo grado di convalida. Poiché la Merkle root incapsula

tutte le transazioni, è possibile verificare in seguito se una transazione è stata inclusa in un determinato blocco. Questo ha un costo: l'utente deve comunque affidarsi a una terza parte per ottenere le informazioni necessarie. Detto questo, i light client sono preferibili a un sistema in cui gli utenti non effettuano alcuna verifica.

I blocchi vengono disposti uno sopra l'altro, con il primo blocco come base, e crescono in altezza (Block height).

Il primo blocco della catena è noto anche come "blocco genesi". Gli strati e la storia profonda di ogni sequenza sono uno degli elementi che rendono Bitcoin così sicuro.

Nell'ambito di un esercizio di mining standard, il block header viene ripetutamente modificato dai miner alterando il valore nonce. Attraverso questo esercizio, si effettua la Proof of Work, che aiuta i miner a essere ricompensati per il loro contributo al funzionamento regolare ed efficiente del sistema blockchain.

Il Block Header contiene tre serie di metadati del blocco. Si tratta di una stringa lunga 80 byte, composta dal numero di versione di Bitcoin lungo 4 byte, dall'hash del blocco precedente lungo 32 byte, dalla Merkle root lunga 32 byte, dal timestamp del blocco lungo 4 byte, dal difficulty target del blocco lungo 4 byte e dal nonce usato dai miner lungo 4 byte.

Componenti del Block Header Ognuno di questi componenti è fondamentale per creare un'intestazione accurata e affidabile.

L'identificatore principale di ogni singolo blocco è l'hash crittografico che contiene. Si tratta essenzialmente di un'impronta digitale, che viene creata eseguendo due volte l'hashing del Block Header attraverso l'algoritmo di hashing.

Il numero di versione di Bitcoin è utile per tenere traccia delle modifiche e degli aggiornamenti del protocollo.

L'hash del blocco precedente si collega al blocco precedente o al suo genitore, proteggendo in modo efficace la catena.

La Merkle Tree è costituita da tutti gli hash delle transazioni all'interno della transazione. Non è così complicato come sembra, ogni hash è solo un ulteriore hash.

Il timestamp è incluso in modo che tutti coloro che i partecipanti siano in grado di vedere una registrazione permanente e codificata di quando si è verificato un particolare evento. In genere fornisce la data e l'ora del giorno di quel particolare evento e spesso è abbastanza preciso da rientrare in una frazione di secondo, ma è comunque impostata dal miner quindi non può essere considerata affidabile e a tal proposito vienee effettuata dai nodi una verifica tramite il Median time-past.

Block height

Altezza del blocco

Livello: intermedio

Argomento: tecnologia

È l'indice numerico progressivo del blocco, e corrisponde al numero di blocchi della blockchain quando quel blocco è stato minato. Nella blockchain è l'unico valore che consente di identificare la sequenza temporale dei blocchi, poiché il riferimento temporale (timestamp) inserito nel blocco non può essere considerato accurato.

Block Reward

Ricompensa di blocco

Livello: intermedio

Argomento: tecnologia

Il Block Reward è la ricompensa, un incentivo che viene assegnato al miner che attraverso l'attività di mining riesce ad aggiungere un nuovo blocco nella blockchain.

Contribuendo alla sicurezza e alla crescita della blockchain, il miner ha maggior vantaggio nell'usare le sue risorse per essere ricompensato con questo incentivo piuttosto che cercare di imbrogliare il sistema, garantendo che i miner continuino ad agire nel miglior interesse della blockchain partecipando legittimamente al processo e per la collettività.

La block reward è composta da:

- Block Subsidy: la quantità di nuovi bitcoin coniati in ogni blocco
- Fee sulle transazioni: le commissioni che vengono pagate da chi effettua le transazioni

Poiché la block reward è quasi interamente costituita dal block subsidy, è molto comune vedere le persone parlare del block subsidy riferendosi ad esso come la block reward. Quindi, nella terminologia popolare, generalmente il termine "block reward" non tiene conto delle fee.

Nel caso di Bitcoin, il block subsidy è iniziato a 50 BTC e viene ridotto a metà ogni 210.000 blocchi (circa una volta ogni quattro anni). Questo dimezzamento del subsidy è noto come Halving.

La block reward viene pagata nella transazione coinbase di ogni blocco. Tipicamente, la transazione coinbase è la prima transazione ad essere aggiunta in un blocco, e fondamentalmente genera monete dal nulla perché le monete provengono da un singolo input vuoto.

L'output di una transazione coinbase non può essere speso per 100 blocchi, quindi i miner possono spendere la loro block reward solo dopo un cooldown di 100 blocchi.

Poiché i block subsidy sono dimezzati ogni quattro anni, le fee diventeranno lentamente una parte maggiore della block reward, e questa variazione nella capacità della quantità di denaro che viene destinata alla sicurezza della rete Bitcoin, definita Security budget, ha acceso una discussione sulla sua evoluzione e su eventuali rischi.

La prima volta nella quale nel Block Reward le fee hanno superato il Block Subsidy è stato a maggio 2023, con il blocco 788695: 6,701 bitcoin di fee contro i 6,25 bitcoin del Block Subsidy.

Block Size

Dimensione del blocco

Livello: base

Argomento: tecnologia

La Block Size o dimensione del blocco descrive la quantità di dati che un blocco può occupare, misurata in byte.

I miner non sono autorizzati a creare un blocco con più dati di quelli consentiti dal limite della dimensione del blocco, limitando il numero di transazioni che i miner possono inserire in ogni blocco.

Questo limite viene stabilito per assicurare che la blockchain non cresca troppo rapidamente in dimensioni, il che renderebbe problematico ad un utente medio di essere in grado di mantenere una copia della blockchain e interrogare la blockchain, compromettendo la decentralizzazione.

Il limite della dimensione del blocco è anche la ragione per cui i miner raccolgono le fee o commissioni di transazione basate sulla dimensione dei dati della transazione. I miner cercano di massimizzare le commissioni totali che possono raccogliere per blocco.

Prima dell'attivazione di SegWit, un blocco della blockchain Bitcoin era strettamente limitato ad un massimo di 1MB.

Dopo SegWit, a partire da Bitcoin Core 0.13.0 (rilasciato ad agosto 2016) i blocchi sono misurati in base al peso o weight unit, piuttosto che alla dimensione. Ogni weight unit rappresenta 1/4.000.000 della dimensione massima di un blocco. Un vByte equivale a 4 weight unit, o unità di peso, e quindi un blocco è limitato a 1 vMegabyte, ovvero 4 milioni di weight unit.

La dimensione massima possibile di un blocco dopo SegWit è ora di 4 MB, o meglio 4 milioni di weight unit, che corrispondono a 1 vMegabyte, e adesso si preferisce utilizzare il termine Block Weight o Peso del blocco invece di Block

Size, termine che richiama il periodo di grandi contrasti sul tema della scalabilità noto come Blocksize War.

Fino a quando le Ordinal Inscription non hanno guadagnato popolarità nel 2023, il numero massimo di transazioni che venivano inserite in un blocco tendeva a raggiungere un picco compreso tra 375.000 e 400.000 al giorno, con i blocchi pieni che contenevano tipicamente intorno a 2500 transazioni.
Con l'arrivo delle Ordinal Inscription si è visto un incredibile aumento del numero di transazioni confermate giornaliere, superando le 550.000 al giorno con blocchi pieni che contengono oltre 6 mila transazioni.

Bitcoin Core 29.0 e il limite di 3,992,000 WU Con il rilascio di Bitcoin Core 29.0 ad aprile 2025, introduce un nuovo limite massimo per il peso dei blocchi che i nodi accetteranno e trasmetteranno (relay). Questo nuovo limite è leggermente inferiore al limite teorico di 4,000,000 WU, precisamente 3,992,000 WU.

A causa di un bug, il peso riservato predefinito per l'header del blocco a dimensione fissa, il conteggio delle transazioni e la transazione coinbase (4.000 WU) veniva riservato due volte e non poteva essere ridotto. Di conseguenza, il peso totale riservato era sempre di 8.000 WU, il che significava che anche specificando un -blockmaxweight superiore al valore predefinito (fino al massimo di 4.000.000 WU), la dimensione effettiva del blocco non avrebbe mai superato i 3.992.000 WU. La correzione consolida la riserva in un unico punto e introduce una nuova opzione di avvio, -blockreservedweight, che specifica direttamente il peso riservato. Il valore predefinito di -blockreservedweight è impostato a 8.000 WU per garantire la retrocompatibilità per gli utenti che si affidavano al comportamento precedente di -blockmaxweight. Il valore minimo di -blockreservedweight è impostato a 2.000 WU. Gli utenti che impostano -blockreservedweight al di sotto del valore predefinito dovrebbero assicurarsi che il peso totale dell'header del loro blocco, del conteggio delle transazioni e della transazione coinbase non superi il valore ridotto, altrimenti potrebbero rischiare di minare un blocco non valido.

block storm

tempesta di blocchi

Livello: avanzato

Argomento: tecnologia

Un block storm, o tempesta di blocchi, si verifica quando la blockchain viene inondata da numero insolitamente elevato di blocchi.

Un block storm può provocare la creazione di 10 o 20 mila blocchi in un solo giorno, rispetto ai circa 144 blocchi al giorno che dovrebbero essere creati in media ogni 10 minuti in condizioni normali.

Condizioni estremamente improbabili sono necessarie affinché un block storm si verifichi sulla mainnet.

Block storm sulla testnet Sulla testnet a causa del bug time-warp, i block storm si verificano con maggiore probabilità, e possono avvenire in modo naturale o artificioso.

Su una testnet, un block storm può verificarsi in modo naturale circa due volte all'anno.

Per creare le condizioni di un block storm nella testnet devono coincidere due eventi:

- **minimum difficulty rule** (regola della difficoltà minima): se sulla testnet non viene trovato alcun blocco per 20 minuti, la difficoltà si reimposta automaticamente al minimo per un singolo blocco
- **blocco del retarget**: l'algoritmo di regolazione della difficoltà (DAA, difficulty adjustment algorithm) regola la difficoltà ogni 2016 blocchi, in un blocco chiamato blocco del retarget

Secondo la distribuzione di Poisson del mining, circa il 12% dei blocchi impiega più di 20 minuti ad essere minato, questo sia sulla mainnet che sulla testnet. Tuttavia, sulla testnet, i 20 minuti che attivano la regola della difficoltà minima possono coincidere con il blocco retarget.

Quando questi due eventi coincidono e la difficoltà viene impostata al minimo nel blocco del retarget, tale bassa difficoltà non rimane solo per un blocco, ma viene mantenuta per un periodo più lungo. Di conseguenza, i miner partecipanti con tale difficoltà molto bassa mineranno molti blocchi in periodi molto inferiori ai 10 minuti.

I block storm possono anche essere provocati deliberatamente monitorando la rete e creando le condizioni necessarie, causando uno stato continuo di block storm sulla testnet. Questo comportamento è considerato un griefing attack, e eseguirlo risulta decisamente semplice, come dimostrato da diversi casi documentati.

Block Subsidy

Livello: intermedio

Argomento: tecnologia

La Block Subsidy, letteralmente la sovvenzione del blocco, è la quantità di nuovi bitcoin coniati in ogni blocco. Ogni blocco che viene prodotto e aggiunto alla blockchain permette al miner creatore del blocco di coniare una certa quantità di nuovi bitcoin.

Questa quantità è strettamente determinata da un algoritmo nel codice sorgente di Bitcoin chiamato Halving: è iniziato con 50 BTC per blocco, e viene

dimezzato ogni 210.000 blocchi o circa 4 anni.

Il block subsidy è il modo in cui i nuovi bitcoin entrano in circolazione, e ha quindi un impatto sull'inflazione.

Il block subsidy viene pagato nella transazione coinbase di ogni blocco. Questa transazione speciale è la prima transazione in ogni blocco, e non ha input. L'output di una transazione coinbase non può essere speso per 100 blocchi, quindi i miner possono spendere il loro block subsidy solo dopo un periodo di 100 blocchi chiamato Cooldown.

Ogni blocco contiene molte transazioni, ognuna delle quali ha delle fee, o commissioni, per incentivare i miner ad inserirli nel blocco. La somma del block subsidy e delle fee cumulative delle transazioni in un blocco produce il Block Reward, la ricompensa di blocco.

Il Block Reward incentiva i miner a rimanere onesti e presentare blocchi validi, e poiché il block subsidy diminuisce della metà ogni quattro anni, si teorizza che il block reward sarà fatto sempre più dalle fee e sempre meno dal block subsidy e su questo si è aperta una discussione sulla sostenibilità di questo modello o Security budget.

block template

Livello: avanzato

Argomento: tecnologia

Un block template, modello di blocco, è una lista di transazioni non confermate, solitamente ottimizzate in base alle fee più profittevoli, limitate dalle dimensioni del blocco.
Queste transazioni sono utilizzate da una mining pool nella costruzione di un nuovo blocco ancora da minare.
Per massimizzare la block reward, la ricompensa del blocco, il template include i pacchetti di transazioni che pagano la fee più alta.

La chiamata di procedura remota (RPC) di Bitcoin Core chiamata **getblocktemplate** viene utilizzata periodicamente per richiedere un nuovo block template. Alcune mining pool potrebbero utilizzare anche la RPC di Bitcoin Core, mentre altri potrebbero avere implementato i propri algoritmi di selezione delle transazioni e infrastrutture per la creazione del template.

Le mining pool aggiornano il loro block template appena vengono a conoscenza che sia stato minato un nuovo blocco. Inoltre, la maggior parte delle mining pool pubbliche aggiorna il proprio block template circa ogni 30 secondi per includere nei propri blocchi le transazioni appena ricevute.

Le attività Stratum non contengono l'elenco completo delle transazioni incluse nel template del blocco.

Un miner che partecipa al mining tramite una mining pool, deve solo costruire un block header, operazione che può essere eseguita senza conoscere tutto il contenuto del template. I miner attualmente esauriscono velocemente il nonce a 32 bit nel block header e possono quindi aggiornare il timestamp nell'header, modificare la versione alla maniera dell'overt ASICBoost o cambiare il cosiddetto extranonce nella transazione coinbase, il che provoca un cambiamento della merkle root. Per fare ciò, i miner hanno bisogno della transazione coinbase, delle informazioni sull'extranonce e dei merkle tree per calcolare una nuova merkle root.

L'elenco dei merkle tree nelle attività Stratum contiene solo le informazioni necessarie per calcolare la merkle root. Per costruire la merkle root, la transazione coinbase viene hashata insieme al primo merkle tree, il risultato viene quindi hashato con il secondo merkle tree, che a sua volta viene hashato con il terzo merkle tree. La merkle root viene raggiunta una volta che tutti i merkle tree sono stati hashati insieme.

Con il protocollo Stratum V2 il miner partecipa in modo più diretto alla costruzione del block template, dichiarando le transazioni alla pool che può quindi scegliere di accettarle o rifiutarle.

Block Weight

Peso del blocco

Livello: avanzato

Argomento: tecnologia

Block weight o peso del blocco è una misura della dimensione di un blocco, misurata in weight unit o unità di peso.

Il protocollo Bitcoin limita i blocchi a 4 milioni di weight unit, limitando il numero di transazioni che un miner può includere in un blocco. Quattro milioni di weight unit equivalgono a 4 MB di dati, il che significa che la dimensione massima di un blocco è ora di 4 MB.

Questo limite è stato posto per evitare che la blockchain cresca troppo velocemente, impedendo ai singoli utenti di gestire un nodo e di convalidare completamente la blockchain, cosa che a sua volta danneggerebbe la decentralizzazione di Bitcoin.

Il Block weight è stato implementato come misura per i limiti di blocco con l'aggiornamento SegWit. Prima di Segwit, il limite di blocco era di 1 MB, misurato in byte, e veniva chiamato Block Size o dimensione del blocco.

La motivazione dell'utilizzo di un unico vincolo composito, invece di due limiti separati come 1MB di dati di base e 3MB di dati del witness, e dovuto al fatto che l'utilizzo di due limiti separati renderebbe quasi impossibile la stima di mining e fee. I miner dovrebbero risolvere un complesso problema di ottimizzazione

non lineare per trovare l'insieme di transazioni che massimizzano le fee in base a entrambi i vincoli, e i wallet non sarebbero in grado di sapere cosa pagare, poiché dipende da quale delle due condizioni è più vincolata dal momento in cui i miner cercano di produrre blocchi con le loro transazioni. Un altro problema di questo approccio è il freeloading. Una volta che un insieme di transazioni raggiunge il vincolo di 1 MB di dati di base, si possono aggiungere fino a 3 MB di dati supplementari al witness aumentando solo minimamente la fee. In questo caso, il costo marginale per lo spazio extra del witness diventa effettivamente pari a zero.

Blockchain

Catena di blocchi

Livello: base

Argomento: tecnologia

Il termine blockchain è un composto dal termine inglese block, che significa 'blocco', e dal termine chain, che significa 'catena'. La blockchain è quindi una serie di blocchi collegati tra loro a formare una catena.

Il collegamento tra i blocchi della catena avviene inserendo in ogni nuovo blocco l'hash del blocco precedente. Questo hash è una funzione matematica che trasforma i dati in una stringa di caratteri univoca e irreversibile. Per modificare un blocco, è necessario modificare anche l'hash del blocco, e questo richiederebbe la modifica di tutti i blocchi successivi. In questo modo, anche grazie alla proof-of-work, la blockchain è resistente alla modifica dei dati.

L'origine del concetto blockchain è attribuito a Satoshi Nakamoto con la creazione di Bitcoin, anche se nel suo white paper il termine *blockchain* non è presente nenche con i termini "*block chain*" separati: viene utilizzato il termine chain da solo, o eventualmente per lo più associato a proof-of-work (*proof-of-work chain*), e a volte anche ad hash (*chain of hash-based proof-of-work*), o firme digitali (*chain of digital signatures*), e associato a block solo due volte in "*blocks are chained*" e "*chain of blocks*".

Dopo alcuni anni dal lancio di Bitcoin, hanno iniziato a proliferare sempre più progetti che, enfatizzando l'aspetto tecnologico e cercando di separarlo da Bitcoin, hanno creato un fortissimo hype del termine blockchain, quasi a prendere le distanze da Bitcoin.

Decine di migliaia di progetti che hanno cercato e continuano a cercare di presentarsi come alternative a Bitcoin, altcoin che con il motto "*blockchain si ma Bitcoin no*" hanno proposto le più fantasiose e a volte improbabili "evoluzioni" a Bitcoin:

- sostituzione del meccanismio di consenso proof-of-work con altri quali POS o Proof-of-Stake, Proof-of-Authority, PoB,PoC, PoET, …

- sostituzione del concetto di permissionless con quello di Blockchain Private o Federate

Una blockchain dovrebbe essere resistente alla modifica dei dati, alla censura, aperta e distribuita, e registrare le transazioni in modo verificabile e permanente, cose che le proposte alternative a Bitcoin non hanno fatto con la stessa efficacia. Così, queste alternative, nel corso degli anni hanno avuto l'effetto di convalidare e confermare l'unicità e la superiorità di Bitcoin, in tutti quegli aspetti che erano stati criticati.

È stato proposto nel corso del tempo di utilizzare il termine time-chain invece di blockchain, anche in riferimento al concetto di Timestamp server introdotto nel white paper di Nakamoto, mediante il quale la blockchain è una catena temporale che utilizza il server di timestamp per generare una prova computazionale dell'ordine cronologico delle transazioni: ogni timestamp include il timestamp precedente nel suo hash, formando una catena, con ogni timestamp aggiuntivo che rafforza quelli precedenti.
Tuttavia, va notato che il timestamp inserito dai miner nei blocchi non è un timestamp preciso e non deve necessariamente essere sequenziale tra un blocco e l'altro. A tale scopo, si è dovuti ricorrere al concetto di median time-past per stabilire un controllo di congruenza nell'impostazione dei timestamp dei blocchi.

Blocksize War

Livello: intermedio

Argomento: politica

La comunità Bitcoin è conflittuale, e sulle proposte alla modifica del protocollo ci sono state delle controversie intense.

Probabilmente quella più importante, e che ha lasciato il segno, è nota come Blocksize war.

Si è svolta tra il 2015 e il 2019, e ha visto la comunità dividersi in small-blocker che si opponevano ad ingrandire la dimensione dei blocchi della block chain bitcoin, e big-blocker che proponevano di aumentare la dimensione dei blocchi per scalare bitcoin.

Il 15 luglio 2010, Satoshi aggiunse la seguente riga di codice al repository del software:

```
static const unsigned int MAX_BLOCK_SIZE = 1000000;
```

Il software contenente questo aggiornamento venne rilasciato il 19 luglio 2010. Il nuovo limite di 1 MB non entrò in vigore fino al 7 settembre 2010, all'altezza del blocco 79.400 (79.400 blocchi dal lancio di Bitcoin).

All'epoca i blocchi più grandi erano di pochi kilobyte.

Satoshi non fornì una ragione chiara per aver posto questo limite alla dimensione del blocco.

Secondo Gavin Andresen, lo sviluppatore che ha ricevuto il testimone dello sviluppo bitcoin direattamente da Satoshi Nakamoto, si trattava di impedire ai miner di eseguire un attacco DDoS e che doveva essere solo una misura temporanea. Ma persone come Gregory Maxwell hanno suggerito che si trattava di un limite permanente per evitare che la blockchain diventasse troppo grande.

Jeff Garzik propose di eliminare il limite già nel 2010, sostenendo che il limite basso era un "problema di marketing". Theymos evidenziò il rischio di un fork della chain, poiché il software non aggiornato avrebbe rifiutato blocchi di grandi dimensioni.

Satoshi scrisse che i tempi non erano maturi per un aumento, ma che si sarebbe potuto fare codificando la modifica in modo che si applicasse a partire da un timestamp o da un'altezza di blocco futuri (nel suo esempio, il 2011), dando alle persone il tempo sufficiente per aggiornarsi.

Nel periodo 2010-2014 ci furono molte discussioni sul tema; alcuni erano infastiditi dal fatto di dover sostenere il costo dell'archiviazione di gigabyte di spam per sempre creati da applicazioni per il gambling.
E in tale fase vennero introdotti i concetti di soft fork e hard fork. E che "*gli hard fork sono intrinsecamente insicuri e ci sia bisogno di un consenso assolutamente completo per implementarli*".

Nel 2015 Sidechain e Lightning vennero presentati come soluzioni per lo scaling.

Tra il 2014 e il 2015 avvennero i primi veri tentativi di affrontare il limite della dimensione dei blocchi. La prima grande spinta per aumentare il limite arrivò nel maggio 2015, quando Gavin Andressen e Mike Hearn proposero di aumentare il limite di dimensione dei blocchi a 20 MB. Dopo le discussioni con i miner, il limite proposto fu ridotto a 8 MB. In realtà, a quel tempo, qualsiasi dimensione effettiva dei blocchi superiore a 1 MB avrebbe dato grandi vantaggi ai più grandi miner/pool cinesi. Mike Hearn aveva previsto che i manutentori del repo github di Bitcoin Core avrebbero posto il veto a qualsiasi aumento della dimensione dei blocchi e decise di imporre il BIP-101, un blocco da 8 MB con una road map di aggiornamenti futuri tramite un hard fork (XT). La comunità che sosteneva Core reagì negativamente ritenendo che la sua road map per gli aggiornamenti futuri fosse troppo aggressiva.

In quel periodo, la moderazione del sub reddit r/bitcoin, uno dei principali social che accoglieva le discussioni della comunità Bitcoin, ha iniziato ad applicare una più aggressiva politica di moderazione, e ogni discussione su XT venica bollata alla stregua di "*discussione sulle altcoin fuori tema*", radicalizzando ulteriormente le due fazioni.

Molti miner manifestarono un interesse per un aggiornamento a 8 MB di dimensione del blocco senza alcuna tabella di marcia per gli aggiornamenti futuri, anche tramite il BIP-100 che raccolse più del 50% di sostegno da parte dei

miner, ha delineando un modo per i miner di votare sulle modifiche al limite di dimensione dei blocchi.

I limiti di dimensione dei blocchi a 4 MB e oltre probabilmente avrebbero dato ai miner cinesi un vantaggio inaccettabile.

Jeff Garzik presentò il suo piano "2 MB upgrade ASAP" (BIP-102), e anche questo fu respinto.

La situazione rimase a lungo in stallo, con numerose diverse proposte.

Blockstream, il MIT e altri proposero il workshop Scaling Bitcoin. Erano consentiti solo discorsi tecnici, nessuna "politica", nessuna decisione; qualsiasi richiesta di aumentare il limite di dimensione dei blocchi era specificamente off-topic.

A Peter R. Rizun è stato permesso di tenere un discorso alla conferenza di Montreal del settembre 2015 in cui si diceva che il limite di dimensione dei blocchi poteva essere tranquillamente rimosso, ma non è stato invitato alla successiva conferenza di Hong Kong del dicembre 2015.

Peter R Rizun e Andrew Stone iniziarono a lavorare su Bitcoin Unlimited (rilascio iniziale gennaio 2016).

Peter Wuille presentò SegWit al workshop Scaling Bitcoin di Hong Kong nel dicembre 2015, e in un primo momento è stato etichettato come un "aumento della dimensione dei blocchi di 4 volte attraverso un softfork" - anche se questo non ha retto all'esame, e nelle diapositive l'aumento della capacità per una transazione normale è dato a 1,75 volte. La tabella di marcia per la scalabilità di Bitcoin Core è stata redatta e conteneva molte ottimizzazioni, che rendevano il software di Bitcoin Core meno esigente in termini di risorse (e quindi rendevano più sicuro l'aumento della capacità).

Ma l'unica promessa di aumento della capacità era l'aumento teorico di ~1,7x offerto da SegWit.

Il 2016 fu l'anno del lungo stallo. Nella conferenza Hong Kong Roundtable Consensus si raggiunse un accordo su una tabella di marcia con SegWit prima e un aumento della dimensione dei blocchi di 2 MB poi. Alcuni considerarono l'accordo nullo già pochi giorni dopo la sua stipula. Con il gruppo di Bitcoin Core che negava di supportare un aumento della dimensione dei blocchi e i miner che negavano di implementare SegWit prima di ricevere la promessa di un aumento della dimensione dei blocchi, ci fu uno stallo di lunga durata.

Gavin Andressen tentò di imporre un aggiornamento "di compromesso" di 2 MB (BIP-109) attraverso il suo fork di Bitcoin Classic, tentativo che non solo non andò a buon fine, ma portò anche ad un allonanamento di Andressen. Con la morte di BIP-109, ci fu la spinta per il "consenso emergente" come implementato in Bitcoin Unlimited. Alla fine, la maggior parte dei big-blocker si è trovata d'accordo nel sostenere Emergent Consensus, che a un certo punto ottenne quasi il 50% di consenso da parte dei miner.

2017: UASF, SegWit2X, ASICBOOST, Bitcoin Cash Gli small-blocker cominciarono ad arrabbiarsi per la mancata attivazione di SegWit da parte dei miner; la tesi sostenuta era che le fee elevate e i problemi di congestione fossero dovuti al fatto che i miner privassero la comunità del tanto necessario aggiornamento di SegWit. Arrivò quindi la proposta di UASF, un tentativo altamente pericoloso di forzare l'aggiornamento di SegWit, definito da alcuni come sybil attack. Chiunque avesse eseguito Bitcoin Core con UASF abilitato avrebbe ignorato i blocchi provenienti da miner che non supportavano SegWit. Con meno del 50% dei miner che supportavano UASF, ci sarebbe stata uno spit della rete, con una rete UASF e una rete non UASF in disaccordo sulla blockchain.

Si scoprì poi che il più grande operatore di mining Bitmain utilizzava un metodo brevettato di "covert asic boost" per effettuare il mining più velocemente, avendo così un vantaggio sugli altri miner che erano anche i suoi stessi clienti. Il metodo utilizzato era incompatibile con SegWit e questo poteva essere motivo dell'ostilità verso SegWit. Dopo aver appreso questa notizia, ci fu uno spostamento della comunità verso gli small-blocker.

A causa della lunga situazione di stallo e con l'imminente disastro dell'UASF che si avvicinava ogni giorno di più, Jeff Garzik e altri proposero il compromesso SegWit2X. Si trattava sostanzialmente di una ripresa dell'accordo della conferenza di Hong Kong. I miner e gli altri principali attori del settore si riunirono e promisero di sostenere l'iniziativa SegWit2X e di utilizzare software alternativi nell'improbabile caso in cui Core non avrebbe supportato l'aggiornamento a 2MB. Il progetto BitcoinABC venne creato come piano di emergenza nel caso in cui UASF sarebbe diventato reale o l'iniziativa SegWit2X avrebbe fallito per altri motivi.

1° agosto, a sorpresa, venne attivato il fork Bitcoin Cash, spinto anche dal fork tra Ethereum e Ethereum Classic che aveva mostrato come un fork potesse consentire a due catene di potersi evolvere indipendentemente dal momento del fork, contraddicendo la regola del whitepaper di Satoshi Nakamoto secondo il quale solo la chain più lunga possa sopravvivere.

Con la paura delle conseguenze dello UASF, i miner decidono di adottare Segwit e l'iniziativa SegWit2X viene abbandonata.

BLS signature

Acronimo di: Boneh-Lynn-Shacham signature

Livello: avanzato

Argomento: tecnologia

La firma digitale BLS, nota anche come Boneh-Lynn-Shacham, è uno schema di firma crittografica che consente a un utente di verificare l'autenticità di un firmatario.

Rispetto alle firme ECDSA o Schnorr, presenta diversi vantaggi evidenti:

- è 2 volte più breve
- è compatibile con l'aggregazione di firme e chiavi
- è deterministico: non si basa sui generatori di numeri casuali

A causa dei suoi requisiti minimi di archiviazione e larghezza di banda, è stato adottato da diverse blockchain come Ethereum, Dfinity, Algorand e Chia, e può essere implementato nativamente su Bitcoin.

Lo schema utilizza un accoppiamento bilineare per la verifica e le firme sono elementi di un gruppo di curve ellittiche.

Le firme prodotte dallo schema di firma BLS sono spesso chiamate firme brevi, firme brevi BLS o semplicemente firme BLS. Lo schema di firma è dimostrabile come sicuro (lo schema è esistenzialmente non falsificabile sotto attacchi adattivi di tipo chosen-message) nel modello di oracolo casuale, assumendo l'intrattabilità del problema di Diffie-Hellman computazionale in un gruppo di Diffie-Hellman gap.

Boating accident

Incidente in barca

Livello: base

Argomento: legale

Se avete molti amici bitcoiner, rimarrete sicuramente sopresi da quanti di loro vi diranno di aver avuto un incidente in barca. E immancabilmente, in questi incidenti in barca sono andate perse le chiavi private dei loro bitcoin.

Stiamo parlando di bitcoiner che non si affidano a servizi custodial per conservare i propri fondi. Questi bitcoiner hanno un wallet non custodial, non fiduciario, hanno il vantaggio che non c'è nessun terzo che può accedere alle loro informazioni o modificarle, ad esempio sequestrando i fondi o imponendo regole per ritirare i propri fondi. In poche parole, questi bitcoiner controllano le loro chiavi private. E così hanno il pieno controllo dei loro fondi e fintanto che le chiavi private sono conosciute solo da loro, i loro fondi non possono essere bloccati o sequestrati.

Ora, la prima regola di un bitcoiner è non parlare mai dei propri bitcoin, ma cosa succede se qualche malintenzionato impositore di balzelli vuole aggredire il patrimonio del nostro povero bitcoiner, e magari in qualche modo riesce a conoscere l'indirizzo pubblico del suo wallet, e può vedere quanti sudati sats ci sono conservati?

Essere un bitcoiner significa anche avere la libertà di possedere le chiavi private senza dover rendere conto a nessuno, e può anche accadere che tu possa perderle e nessuno può sostenere che tu abbia ancora quei bitcoin. L'incidente in barca

è quello dove tu avresti (ovvero dici di aver) perso le chiavi private e quindi non sei più in possesso di quei bitcoin.

Questo modo di dire è mutuato dal possesso di armi, per le quali una legge ne imponeva la registrazione della perdita; in un processo un agente era stato assolto dall'accusa della mancata registrazione adducendo la motivazione della perdita appunto in un incidente in barca, e da questo precedente viene utilizzata tale motivazione che se può essere valida per un agente deve esserlo per tutti.

BOLT

Acronimo di: Basis of Lightning Technology

Livello: avanzato

Argomento: tecnologia

Così come su internet ci sono le RFC e su bitcoin le BIP, su Lightning Network ci sono i BOLT che definiscono gli standard di interoperabilità e le specifiche che si possono trovare su lightning-rfc su github. Le BOLT sono documenti molto tecnici che descrivono non solo cos'è il tutto, ma esattamente come funziona tutto.

Le BOLT sono specifiche che descrivono le regole di consenso e gli standard della rete Lightning. Gli standard stabiliti dai BOLT consentono a diverse implementazioni Lightning come LND e c-lightning di integrarsi e formare una rete. Man mano che il Lightning Network continua a svilupparsi, i BOLT vengono adattati e migliorati.

Esistono anche le bLIP, Bitcoin Lightning Improvement Proposal, documenti di progettazione che descrivono nuove funzionalità che quando sono destinate a diventare universali o quasi, devono essere BOLT.

BOLT11

Livello: avanzato

Argomento: tecnologia

Bolt 11 definisce il formato per una invoice, o richiesta di pagamento, per Lightning Network.

È un modo per inviare Bitcoin sulla rete Lightning. È un URL che contiene tutte le informazioni necessarie per inviare un pagamento Lightning, come l'importo, l'indirizzo del destinatario e l'ID di rete.

Un esempio di una invoice BOLT11 potrebbe apparire così:

lnbc15u1p3xnhl2pp5jptserfk3zk4qy42tlucycrfwxhydvlemu9pqr93tuzlv9cc7g3sdqsvfhkcap3xyhx7un8cqzpgxqzjc

Ecco una spiegazione delle diverse parti:

- **lnbc**: Questo è il prefisso standard che indica che si tratta di una invoice Lightning Network (Lightning Network Bitcoin).
- **15u**: Questo è l'importo della invoice in satoshi. In questo caso, "15u" rappresenta 15 satoshi. La "u" sta per "microbitcoin," che è una sottomultiplo di Bitcoin.
- **1p3xnhl2** è il timestamp, che decodificato corrisponde al valore 1651105770, ovvero 28 aprile 2022 00:29:30
- **pp5jptserfk3zk4qy42tlucycrfwxhydvlemu9pqr93tuzlv9cc7g3s** tag:p, è il payment_hash
- tag d: **dqsvfhkcap3xyhx7un8** è la descrizione che in questo esempio decodificata corrisponde alla stringa "bolt11.org"
- tag c: **cqzpg** min_final_cltv_expiry Data: 40 indica il valore minimo che il pagatore deve utilizzare per il campo cltv_expiry il numero di blocchi che devono passare prima che i fondi possano essere recuperati in caso di dispute o inattività
- tag x: **xqzjc** indica la scadenza (expiry) che decodificato corrisponde a 600
- **sp5f8c52y2stc300gl6s4xswtjpc37hrnnr3c9wvtgjfuvqmpm35evq** tag:s, è il payment_secret
- tag 9: **9qyyssq** feature_bits
- **y4lgd8tj637qcjp05rdpxxykjenthxftej7a2zzmwrmrl70fyj9hvj0rewhzj7jfyuwkwcg9g2jpwtk3wk** è la firma
- **4gj5hs** checksum

Quindi, questa invoice richiede un pagamento di 15 satoshi e include altre informazioni aggiuntive che potrebbero essere utilizzate per scopi di registrazione o descrizione del pagamento. Il Payment Hash viene utilizzato per confermare che il pagamento è stato effettuato con successo una volta che il destinatario riceve il pagamento sulla rete Lightning.

Le Bolt 11 invoices sono state introdotte nel 2018 e sono ora il formato di invoice più comune sulla rete Lightning.

Per creare una Bolt 11 invoice, è necessario un wallet Lightning. Il wallet creerà un URL che contiene tutte le informazioni necessarie per inviare un pagamento Lightning. L'URL può quindi essere condiviso con il destinatario, che può quindi utilizzare il proprio wallet Lightning per inviare il pagamento.

Quando un destinatario invia un pagamento a una Bolt 11 invoice, il pagamento viene inviato alla rete Lightning. Il pagamento viene quindi instradato all'indirizzo del mittente. Una volta che il pagamento arriva al destinatario, viene accreditato sul suo wallet Lightning.

Le Bolt 11 invoices sono uno strumento importante per la rete Lightning. Consentono agli utenti di inviare e ricevere Bitcoin sulla rete Lightning in modo efficiente, facile e compatibile.

BOLT12

Livello: avanzato

Argomento: tecnologia

BOLT12 è una proposta di standard per Lightning Network, che aggiunge diverse funzionalità alle Lightning Invoice.

BOLT 12 introduce le **offer**, o offerte, nella rete Lightning.

Le offer sono un precursore dell'Invoice e consentono funzionalità chiave come i codici QR riutilizzabili, la possibilità di inviare e ricevere pagamenti e una maggiore privacy.

Attraverso un unico codice QR, una offer consente di prelevare l'invoice da un nodo lightning in modo da preservare la privacy, consentendo anche cose come richiedere che un nodo remoto paghi la invoice.

I codici QR riutilizzabili aprono la strada a casi d'uso come abbonamenti e donazioni ricorrenti. Le funzionalità di invio e ricezione possono essere utilizzate per i bancomat Lightning e i rimborsi privati. Infine, nuove funzionalità come Route blinding (chiamato anche Blinded Paths), payer key e le firme Schnorr forniscono un ulteriore livello di privacy.

È composto da caratteristiche diverse e diversi pezzi messi insieme per realizzare cose diverse: codici QR statici, invoice modulari, privacy per la persona che riceve il pagamento.

Questo BOLT specifica un protocollo in cui il beneficiario fornisce un URL di pagamento a uno o più potenziali pagatori.

I pagatori possono utilizzare l'URL per aprire un canale di comunicazione al beneficiario per richiedere le invoice. È possibile accedere allo stesso URL più volte e può essere utilizzato da più pagatori per più pagamenti. L'URL è in genere abbastanza breve da poter essere inserito in un codice QR

Bond

Obbligazione

Livello: intermedio

Argomento: finanza

E' un titolo di credito emesso da società o enti pubblici come lo Stato o una municipalità per raccogliere denaro a debito. E' un piano di rimborso prevedibile e strutturato in cui l'emittente riceve un investimento per un periodo di tempo specificato in cambio di un rendimento. Le obbligazioni generalmente maturano dopo un periodo di cinque, dieci o venticinque anni e mantengono tassi di interesse fissi. Ogni bond ha diverse caratteristiche che lo definiscono. A novembre

2021, l presidente di El Salvador, Nayib Bukele, ha annunciato l'emissione di un bond legato ai Bitcoin, chiamato Vulcano Bond

border wallet

Livello: intermedio

Argomento: tecnologia

I Border Wallet sono un'ottima soluzione per coloro che hanno difficoltà a memorizzare le Seed Recovery Phrase a causa della loro complessità o del rischio di perderle o dimenticarle.

I Border Wallet forniscono un metodo per memorizzare le Seed Recovery Phrase utilizzando tre componenti:

- **Entropy Grid** o Griglia di Entropia: una griglia di tutte le 2048 parole del seed distribuite in modo casuale.
- **Pattern**: una sequenza o schema visuale generato dall'utente.
- **La Parola Finale "Numero"**: L'ultima parola del seed (checksum).

Combinati, questi tre componenti costituiscono il tuo Border Wallet.

EGG Entropy Grid Generator Utilizzando il generatore di griglie di entropia (EGG), gli utenti possono generare la propria griglia casuale e sicura da un punto di vista entropico di tutte le 2048 parole del seed definite dal BIP39 e poi applicare un modello memorabile o un insieme di coordinate delle celle ad essa - che solo loro conoscono - al fine di creare un wallet.

Poiché ogni griglia di entropia unica contiene un elenco completo di tutte le parole seed del BIP39 distribuite in modo casuale e i modelli degli utenti esistono solo nella loro mente, gli utenti memorizzeranno la loro griglia di entropia (o la sua frase di ripristino) fisicamente o digitalmente.

Calcolatore della parola finale e la parola finale "Numero" EGG consente agli utenti di importare le 11 o 23 parole pertinenti dalla loro griglia di entropia per calcolare la parola finale di controllo, o checksum. Oltre al pattern dell'utente, il checksum è l'unica cosa che deve essere memorizzata.

Tuttavia, per rendere ancora più facile il processo, EGG include una caratteristica unica di "numero di parola finale". Con questo, invece di dover ricordare la parola "pair", gli utenti possono semplicemente ricordare il numero "5" - potrebbero persino scrivere questo numero sulla loro griglia di entropia poiché, da solo, non ha alcun significato e non fornisce alcun suggerimento sulla parola finale senza che siano note le altre parole.

Gli utenti possono anche cambiare la parola finale Numero in qualcosa di più significativo per loro, anche se ciò cambia anche la parola finale stessa. Pertanto,

se gli utenti cambiano il numero, il nuovo checksum mostrato deve essere utilizzato per impostare il loro Border Wallet. Non è consigliato cambiare il numero (poiché viene generato con entropia dallo strumento), ma l'opzione è disponibile se desiderata.

Bot

Livello: intermedio

Argomento: finanza

I bot, o per esteso cryptocurrency trading bot, robot per il trading di criptovalute, sono programmi per computer che acquistano e vendono automaticamente varie criptovalute secondo dei parametri preimpostati con l'obiettivo di generare un profitto dalle oscillazioni dei prezzi.

brainwallet

Livello: intermedio

Argomento: tecnologia

NON utilizzare un brainwallet. È probabile che tu perda i tuoi fondi. Gli esseri umani sono pessimi nell'essere originali. VERAMENTE pessimi nell'essere casuali. E pessimi nel comprendere numeri enormi.

Un brainwallet è un metodo per generare una chiave privata utilizzando una frase segreta che può essere facilmente memorizzata.

La frase segreta viene convertita in una chiave privata attraverso l'uso di un algoritmo di hash o di derivazione delle chiavi, come ad esempio SHA256.

Questo metodo è considerato estremamente insicuro e non dovrebbe essere utilizzato. Gli esseri umani non sono una buona fonte di entropia, il che significa che gli indirizzi Bitcoin generati da frasi chiave di brainwallet sono vulnerabili ad attacchi brute force. Inoltre, esistono database contenenti indirizzi Bitcoin derivati da frasi chiave di brainwallet deboli o compromesse.

Un'altra critica riguarda la sicurezza a lungo termine degli account generati con brainwallet. Sebbene siano protetti dagli hacker online e dai furti fisici, c'è il rischio che il proprietario dimentichi la frase segreta o che venga persa in caso di decesso del titolare.

Di conseguenza, i brainwallet non sono consigliati come opzione sicura per conservare criptovalute.

È importante notare che il concetto di brainwallet non dovrebbe essere confuso con la Mnemonic Wordlist e la Seed Recovery Phrase, anche se a volte viene utilizzato come termine generico per indicare anche questi concetti, essi si riferiscono a metodi più sicuri e affidabili per generare e ripristinare le chiavi private dei portafogli di criptovalute.

BRC-20

Livello: intermedio

Argomento: tecnologia

BRC-20 è uno standard sperimentale di implementazione di un protocollo per la creazione di token sulla blockchain di Bitcoin, modellato facendo riferimento ai token ERC-20 di Ethereum, che consente agli utenti di emettere e trasferire token fungibili.
Lo standard è stato introdotto nel marzo 2023 da un analista pseudonimo on-chain conosciuto come Domo.

BRC-20 è un meta-protocollo che sfrutta le Ordinal Inscription per creare dei token i cui dati (balance e altri metadati) sono salvati direttamente sulla chain di Bitcoin sotto forma di file testo in formato json.

Con BRC-20, il processo di creazione inizia con l'Inscription della funzione "deploy" che crea un token BRC-20 e imposta i metadati importanti come il nome del protocollo, il nome della funzione deploy, il ticker, il limite massimo della supply e il limite massimo di token mintabili attraverso l'Inscription.
Successivamente, il token viene mintato con l'Inscription della funzione "mint" che specifica il quantitativo di token che verrà creato.
Infine, il trasferimento di token avviene tramite l'Inscription della funzione "transfer", che richiede un duplice step. In primo luogo, il mittente crea l'Inscription di trasferimento, poi la trasferisce all'indirizzo destinatario.

Il protocollo BRC-20 non è forzato da alcuna regola di consenso in Bitcoin, non è garantito dalla blockchain bitcoin ed è quindi difficile riconoscere e verificare una Inscription "transfer" non valida.
Inoltre, poiché il protocollo BRC-20 non è address-based come Ethereum, la tracciabilità del balance di ciascun indirizzo può risultare complicata.

BRC-20 rispetto all'ERC-20 su Ethereum ha alcune differenze chiave.
Una delle principali differenze è che BRC-20 usa le Inscription invece di smart contract per la creazione dei token. Le Inscription sono un modo per aggiungere dati ai singoli satoshi sulla blockchain di Bitcoin. Questi dati possono essere qualsiasi cosa, come un nome, un numero o un link a un sito web.

BRC-721

Livello: avanzato

Argomento: tecnologia

BRC-721 è uno standard per token Ordinals di Bitcoin, costruito sul protocollo Bitcoin Ordinals, simile al token BRC-20, ma è sviluppato specificamente per NFT, in quanto BRC-20 è progettato per la creazione di token fungibili.

Così come il nome BRC-20 fa riferimento al popolare standard ERC-20 nato su Ethereum per la creazione di token fungibili, analogamente BRC-721 deriva

dallo standard ERC-721 utilizzato per la creazione di NFT su Ethereum.

Il protocollo BRC-721 è stato introdotto per consentire un approccio decentralizzato ai collezionabili digitali ed è simile allo standard ERC-721 sulla rete blockchain di Ethereum. BRC-721 presenta le stesse qualità di ERC-721 e offre un modo sicuro per verificare, gestire, archiviare e trasferire collezionabili digitali sulla rete Bitcoin.

BRC-721E

Livello: avanzato

Argomento: tecnologia

BRC-721E è uno standard nato per consentire il trasferimento degli NFT dalla blockchain di Ethereum agli Ordinal di Bitcoin.

Un blockchain bridge (o cross-chain bridge) consente agli utenti di trasferire asset e dati digitali tra due diverse reti blockchain. L'obiettivo dello standard token BRC-721E è quello di collegare gli NFT da Ethereum a Bitcoin.

Per farlo, come prima cosa gli utenti devono inviare il loro token ERC-721 su Ethereum a un indirizzo burn.

Quindi, devono coniare l'NFT su Bitcoin utilizzando le Ordinal Inscription, attraverso appositi Bridge.
Questo processo impedisce che si creino degli NFT duplicati perché una volta che il token Ethereum è stato bruciato, è considerato collegato a Bitcoin.
Attualmente, i token BRC-721E inscrivono una versione meno dettagliata dell'NFT su Bitcoin con un collegamento al token Ethereum originale.
È possibile, tuttavia, che lo standard del token si evolva per consentire metadati completi in futuro.

Bridge

Livello: avanzato

Argomento: finanza

Il bridge è un protocollo o un servizio centralizzato o decentralizzato che consente di creare una connessione tra due blockchain che normalmente non possono comunicare tra loro. Con l'uso del bridge, è possibile inviare fondi/valore di token/token da una chain all'altra. Questo collegamento non effettua un reale trasferimento di coin o token, ma generalmente vengono bloccati da una chain per essere mintati i loro token equivalenti nell'altra chain. Nel caso dei bridge Bitcoin, i protocolli esistenti di solito bloccano BTC su Bitcoin per coniare o sbloccare un qualche tipo di token su una blockchain remota. Il processo di trasferimento di bitcoin a una chain remota viene chiamato peg-in, e il processo di trasferimento di bitcoin di nuovo alla blockchain Bitcoin (e quindi lo sblocco dei bitcoin bloccati) viene chiamato peg-out.

Broker

Livello: base

Argomento: finanza

Un broker, intermediario o agente di cambio, nel campo dell'economia è una persona e un ente che organizza le transazioni tra un acquirente e un venditore in cambio di una commissione al momento dell'esecuzione dell'affare.

Un broker che agisce anche come venditore o acquirente diventa una parte principale dell'affare.

Brokerage

Livello: base

Argomento: finanza

Un brokerage è un istituto finanziario o società di intermediazione che consente ai propri clienti di acquistare direttamente degli asset.

A differenza degli Exchange, che fanno incontrare acquirenti e venditori, un brokerage reperirà risorse da terze parti e venderà le risorse ai clienti, semplificando la loro esperienza.

Le società di intermediazione sono generalmente soggette a normative basate sul tipo di intermediazione e sulle giurisdizioni in cui operano.

Esempi di agenzie di regolamentazione delle società di intermediazione includono la SEC (US Securities and Exchange Commission) e FINRA (Financial Industry Regulatory Authority), che regolano gli agenti di cambio negli Stati Uniti.

BSA

Acronimo di: Bank Secrecy Act

Livello: avanzato

Argomento: politica

Il BSA, conosciuto anche come Currency and Foreign Transactions Reporting Act, è una legge federale degli Stati Uniti che richiede a MSB, banche e ad altre istituzioni finanziarie, di monitorare e segnalare operazioni sospette ai funzionari federali, di divulgare alle autorità regolamentate registri come le dichiarazioni delle transazioni in valuta e la storia finanziaria dei conti.
La legge è stata introdotta nel 1970 per contrastare i reati finanziari, in particolare il riciclaggio di denaro.
Il BSA autorizza l'Office of the Comptroller of Currency a valutare le attività bancarie e i processi di gestione di banche nazionali, associazioni federali di risparmio, filiali federali e agenzie di banche straniere.

Il BSA espande il Patriot Act e richiede alle istituzioni finanziarie di adottare programmi di identificazione dei clienti accurati. Le istituzioni sono anche tenute a creare programmi completi contro il riciclaggio di denaro AML per soddisfare i requisiti di conformità BSA.

I programmi di conformità BSA includono meccanismi di controllo interno, test indipendenti, formazione del personale e la nomina di un responsabile della conformità antiriciclaggio (AMLCO, Anti Money Laundering Compliance Officer). Le istituzioni conformi alla BSA depositano rapporti con un alto grado di utilità in materia penale, fiscale, di intelligence e antiterrorismo. La BSA richiede anche che le banche rispettino le regole del Know Your Customer KYC.

Per esempio, le istituzioni devono presentare un rapporto di attività sospette (SAR, suspicious activity report) entro 30 giorni dal verificarsi di attività sospette o potenzialmente sospette. Allo stesso modo, i rapporti sulle transazioni in valuta (CTR, currency transaction reports) sono depositati tramite il modulo 112 del Financial Crimes Enforcement Network (FinCEN) per le transazioni in contanti che superano i 10.000 dollari. Le organizzazioni finanziarie sono comunemente tenute a conservare le segnalazioni e i CTR per almeno cinque anni.

Mentre la BSA è stata lodata per la sua efficacia nel combattere il comportamento illegale, è stata criticata per la mancanza di regole che specifichino cosa esattamente è considerato come *transazione sospetta*. Per acquisire l'accesso alle informazioni, le autorità di polizia non hanno bisogno di un ordine del tribunale. La crescente popolarità delle criptovalute ha suscitato dibattiti sul se e come le aziende che si occupano di transazioni che utilizzano nuovi veicoli finanziari, come bitcoin e altcoin, dovrebbero essere obbligate a rispettare il Bank Secrecy Act, ma per molte persone la privacy e la segretezza è una qualità fondamentale delle criptovalute, così come poter gestire le criptovalute sui propri wallet non-custodial invece che essere gestiti da intermediari finanziari come banche ed exchange, e questo non viene visto con favore dal governo federale statunitense che continua a sforzarsi per ottenere maggiore controllo e visibilità alle transazioni bitcoin, citando spesso l'ipotetico aumento nell'uso delle criptovalute per attività illegali.

BTC

Livello: base

Argomento: finanza

BTC è il simbolo o ticker che rappresenta Bitcoin.

Viene a volte utilizzato anche per differenziare Bitcoin dai vari fork. A causa di un problema con le regole ISO sui ticker a volte viene utilizzata la sigla XBT.

BTFD

Acronimo di: Buy The F**king Dip

Livello: intermedio

Argomento: finanza

espressione colorita che indica fiducia anche in un momento di forte discesa dei prezzi, o dip . Viene utilizzato quando un trader consiglia vivamente ad altri di acquistare una valuta digitale che è scesa di valore

Bubble

Bolla

Livello: intermedio

Argomento: finanza

Una bolla indica che c'è un forte entusiasmo che spinge all'acquisto, spesso non motivato da reali condizioni che lo giustificano, e che crea un ciclo al rialz che può "scoppiare" portando ad un crollo del prezzo o correzione

Bull Market

mercato rialzista

Livello: base

Argomento: finanza

Si riferisce a un andamento positivo dei prezzi di un mercato.

È ampiamente utilizzato non solo nello spazio delle criptovalute, ma anche nei mercati tradizionali. Il Bull Market si verifica quando si ha un forte trend rialzista del mercato che presenta prezzi con aumenti significativi in un periodo di tempo relativamente breve.

Rispetto ai mercati tradizionali, i mercati delle criptovalute sono più piccoli e di conseguenza più volatili ed è quindi è abbastanza comune vedere frequenti Bull Run nelle quali si ha un aumento del prezzo del 40% in 1 o 2 giorni.

L'opposto del Bull Market è il Bear Market.

Bull Run

Livello: base

Argomento: finanza

Una bull run, o corsa al rialzo, è un periodo di tempo anche breve durante il quale i prezzi di un asset o delle criptovalute si trovano in una significativa tendenza al rialzo, aumentano in modo significativo e rapido.

Il termine deriva dalla parola bull, o "toro", che rappresenta un mercato in crescita o bear market. Il termine bullish è traducibile in italiano anche come ottimista,

Durante una bull run, gli investitori si sentono ottimisti e i prezzi delle criptovalute possono continuare ad aumentare per un lungo periodo di tempo.

Una bull run può anche mascherare una Bull trap, che sfrutta l'ottimismo degli investitori.

Bull Trap

trappola per speculatori rialzisti

Livello: intermedio

Argomento: finanza

Una Bull Trap, nota anche come trappola per speculatori rialzisti, si verifica durante un trend rialzista quando un falso segnale, spesso generato da un rimbalzo, induce gli speculatori ad aprire posizioni lunghe, o Long Position, pensando che il mercato continuerà a salire.

In realtà si tratta di un'illusione perché il prezzo dell'asset non continua ad aumentare e si verifica invece un'inversione improvvisa, causando una perdita per gli investitori che hanno acquistato.

La Bull Trap può essere causata da speculatori che acquistano grandi quantità di un asset per far aumentare il prezzo temporaneamente, prima di venderlo a un prezzo più alto, lasciando gli investitori con perdite significative.

Identificare una Bull Trap può essere difficile e le conseguenze possono essere pesanti per gli investitori che non riescono a farlo.

Bullish

Livello: intermedio

Argomento: finanza

Indica un trend rialzista, vedi Bull Market, è la convinzione che una criptovaluta aumenterà di valore.

In generale, Bullish si riferisce a un atteggiamento o a una prospettiva che prevede un aumento dei prezzi. Nel mercato delle criptovalute, una persona che è Bullish su una determinata criptovaluta o sul mercato delle criptovalute in generale, crede che i prezzi saliranno in futuro. Questo atteggiamento è contrario a quello di una persona che è Bearish e crede che i prezzi scenderanno.

In sintesi, un investitore Bullish si aspetta un aumento dei prezzi delle criptovalute, per questo è più propenso a comprare o fare long (cioè speculare sull'aumento dei prezzi) le criptovalute invece che venderle.

Termini associati al Bullish sono:

- Bull market: un mercato in crescita, in cui i prezzi stanno aumentando;
- Bull run: un periodo di tempo durante il quale i prezzi delle criptovalute aumentano in modo significativo;
- Bull trap: situazione in cui gli investitori si sentono ottimisti e comprano criptovalute a prezzi elevati, ma poi i prezzi iniziano a scendere, ingannando gli investitori che hanno acquistato in quel momento.

Burning

Livello: intermedio

Argomento: tecnologia

l Burning, nel contesto delle criptovalute, è un processo che rimuove permanentemente un certo numero di token dalla circolazione, rendendoli inaccessibili e inutilizzabili. In pratica, è come se queste monete digitali venissero "bruciate" e scomparissero per sempre.

Come funziona il burning? Di solito, il burning viene eseguito inviando i token a un indirizzo di portafoglio digitale specifico chiamato "indirizzo eater" o "indirizzo di burn". Questi indirizzi sono progettati in modo tale che nessuno possa accedere ai fondi inviati lì, rendendoli di fatto irrecuperabili.

Perché bruciare le criptovalute?

Ci sono diverse ragioni per cui si ricorre al burning:

Controllo dell'inflazione: Riducendo l'offerta totale di una criptovaluta, il burning può aiutare a contrastare l'inflazione e a mantenere stabile o addirittura aumentare il valore dei token rimanenti. Questo meccanismo è simile a quello utilizzato dalle banche centrali quando ritirano dalla circolazione la moneta cartacea.
Aumento della scarsità: Bruciare token aumenta la loro scarsità, il che può renderli più desiderabili e preziosi.
Miglioramento della sicurezza e dell'efficienza della rete: Alcune criptovalute utilizzano il burning come meccanismo per migliorare la sicurezza e l'efficienza della rete. Ad esempio, Ethereum brucia una piccola quantità di ETH per ogni transazione, riducendo il rischio di spam e congestione della rete.
Proof-of-Burn: Alcune criptovalute utilizzano un meccanismo di consenso chiamato "Proof-of-Burn", in cui gli utenti "bruciano" i loro token per ottenere il diritto di validare le transazioni e guadagnare ricompense.

Esempi di criptovalute che utilizzano il burning:

Binance Coin (BNB): Binance, uno dei più grandi exchange di criptovalute al mondo, brucia regolarmente una parte dei suoi profitti in BNB.
Ethereum (ETH): Come accennato in precedenza, Ethereum brucia una piccola quantità di ETH per ogni transazione.
Stellar (XLM): La Stellar Development Foundation ha bruciato oltre 50 miliardi di XLM nel 2019. Il burning è uno strumento importante nell'ecosistema delle criptovalute, utilizzato per una varietà di scopi. Comprendere il concetto di burning è fondamentale per chiunque voglia investire o utilizzare criptovalute.

Buy Wall

muro di acquisto

Livello: avanzato

Argomento: finanza

È il risultato di un singolo ordine di acquisto enorme o della composizione di più ordini di acquisto di grandi dimensioni che vengono inseriti allo stesso prezzo nel portafoglio ordini di un particolare mercato. I muri di acquisto possono essere creati da un individuo benestante, un gruppo di commercianti o di istituzioni. Questo a volte può essere utilizzato dai grossi investitori per creare un sentimento positivo sul mercato, con lo scopo di impedire che una criptovaluta scenda al di sotto di tale valore, poiché la domanda probabilmente supererà l'offerta quando l'ordine verrà eseguito.

Byzantine Generals' Problem

Problema dei generali bizantini

Livello: avanzato

Argomento: tecnologia

Il problema dei generali bizantini è un esperimento mentale che affronta una questione chiave dell'informatica: è possibile formare un consenso in una rete di computer composta da nodi indipendenti e geograficamente distribuiti?

Il problema è stato proposto nel 1982 da ricercatori dello SRI International Research Institute.

Funziona così: ci sono un certo numero di generali bizantini che assediano una città. Possono comunicare solo attraverso l'invio di messaggeri l'uno all'altro. I generali devono concordare un piano d'azione comune: se attaccare la città o ritirarsi. Tuttavia, alcuni dei generali sono traditori e lavorano attivamente contro la formazione di un consenso; il loro numero e la loro identità sono sconosciuti.

La questione posta dal problema è quale algoritmo decisionale i generali dovrebbero utilizzare per elaborare un piano comune - indipendentemente

dall'interferenza dei traditori - e se tale algoritmo esiste o meno.

Secondo l'analisi dei ricercatori, un tale sistema è effettivamente fattibile, ma il numero di generali leali deve rigorosamente superare i due terzi. Ad esempio, in una situazione con tre generali, di cui uno traditore, i leali non possono mai garantire che riusciranno a raggiungere un consenso.

Questo problema è molto rilevante per le criptovalute in quanto sono, in sostanza, sistemi informatici distribuiti: sono composti da nodi di elaborazione delle transazioni che sono indipendenti l'uno dall'altro e da qualsiasi autorità centrale e possono comunicare solo in remoto. Sono i "generali" che hanno bisogno di raggiungere un consenso su quali transazioni sono state effettuate e quando. I nodi hanno il potenziale per fornire dati errati sulle transazioni sia per scelta che per caso e le loro informazioni devono essere risolte.

Bitcoin (BTC) e altre criptovalute risolvono questo problema tramite soluzioni tecniche come gli algoritmi proof-of-work.

candidate block

blocco candidato

Livello: intermedio

Argomento: tecnologia

In Bitcoin, un candidate block o blocco candidato è un blocco che è stato creato da un miner ma non è ancora stato aggiunto alla blockchain.
I blocchi candidati sono creati quando un miner trova una soluzione al problema di hash che è richiesto per creare un nuovo blocco. Una volta che un blocco candidato è stato creato, viene trasmesso a tutti i nodi della rete Bitcoin. I nodi della rete quindi verificano il blocco per assicurarsi che sia valido. Se il blocco è valido, viene aggiunto alla blockchain.

Il processo di creazione di un blocco candidato è chiamato mining.

Ogni nodo della rete Bitcoin verifica il nuovo blocco candidato prima di considerarlo parte della blockchain. Questo processo di verifica aiuta a garantire che i blocchi aggiunti alla blockchain siano validi e non siano stati manomessi.

Un blocco candidato anche una volta aggiunto alla block chain potrebbe essere rimosso, ad esempio in caso di una riorganizzazione della catena.

Dopo un certo numero di blocchi aggiunti alla catena, o conferme, il blocco può essere considerato facente parte definitivamente della blockchain perché la riorganizzazione della catena a partire da quel blocco sarebbe troppo onerosa.

Candlestick

Livello: intermedio

Argomento: finanza

Le candele (candlesticks) sono parte di una metodologia di grafici utilizzata dagli investitori in azioni e criptovalute per mostrare i prezzi storici e in tempo reale di un determinato asset.

È un'immagine grafica a forma di candela che mostra 4 punti di informazione:

- prezzo di apertura,
- prezzo di chiusura,
- massimo,
- minimo.

nell'intervallo di tempo rappresentato.

Le candele sono progettate per visualizzare i prezzi di apertura, massimi, minimi e chiusura (OHLC) di un asset per periodi di tempo specifici (di solito al minuto, all'ora, al giorno, alla settimana e al mese). Tipicamente, le candele verdi indicano un aumento rialzista del prezzo, mentre le candele rosse segnalano una diminuzione ribassista del prezzo. Le candele sono generalmente considerate come il più noto indicatore tecnico utilizzato dagli investitori.

Un grafico a candele è una tecnica di rappresentazione grafica utilizzata per mostrare le variazioni di prezzo nel tempo.

Conosciuto anche come "indicatore principale", può anticipare il trend agendo su modelli di candele principali prima che gli altri trader seguano.

Punti chiave:

Un grafico a candele è un metodo per mostrare i prezzi storici di un asset (ad esempio, criptovaluta), fornendo un buon riassunto del comportamento del prezzo.
È estremamente rilevante nel trading di Bitcoin e criptovalute, poiché i modelli di candele possono indicare inversioni rialziste o ribassiste.
Considerato un indicatore "principale" e non "ritardato", consente di anticipare il trend agendo su modelli di candele principali prima degli altri trader.

Un grafico a candele è un metodo per mostrare i prezzi, ossia apertura, massimo, minimo e chiusura, di un asset per un periodo definito. Si ritiene che i grafici a candele abbiano avuto origine dai commercianti di riso giapponesi nel XVIII secolo e sono ancora uno dei modi più popolari per visualizzare i prezzi dei mercati finanziari.

Notare la differenza tra la candela Bullish (verde) e la candela Bearish (rossa). Quando il prezzo di apertura di una candela è inferiore al prezzo di chiusura, la candela è considerata rialzista, e viceversa.

Le candele forniscono un buon riassunto del comportamento del prezzo durante il periodo considerato. Tutti gli strumenti di grafico consentono di modificare il periodo del grafico a candele, da periodi di un minuto a una settimana o un mese per candela. Ciò consente al trader di visualizzare rapidamente il sentiment di

mercato (usando i colori) e di capire come si sono comportati i prezzi per la durata selezionata.

Poiché le candele illustrano il movimento dell'asset durante il periodo definito, possono indicare visivamente il sentiment rialzista o ribassista, specialmente quando le candele sono considerate come un gruppo. I trader chiamano queste configurazioni "modelli di candele".

La rappresentazione grafica delle candele è estremamente rilevante nel trading di Bitcoin e criptovalute in generale. Imparando come i modelli di candele possono indicare inversioni rialziste o ribassiste, è possibile anticipare il trend agendo su questi indicatori principali prima che gli altri trader seguano.

Poiché le candele utilizzano dati di prezzo grezzi e si aggiornano non appena un periodo è completato, i modelli di candele sono considerati indicatori "principali" e non "ritardati". Questo rende il riconoscimento dei modelli di candele un elemento fondamentale nel tuo arsenale di trading.

Sebbene i grafici a candele possano essere utilizzati anche per analizzare altri tipi di dati, sono stati inizialmente creati come strumento per facilitare l'analisi dei mercati finanziari. Il concetto di candele si dice che abbia origini dai commercianti giapponesi del XVII secolo.

Ad esempio, un grafico di 1 ora è composto da diverse candele, ognuna che illustra un movimento di mercato di 1 ora. Ogni candela mostra i prezzi di apertura e chiusura (corpo della candela), così come i punti di prezzo massimo e minimo (lunghe linee sopra e sotto il corpo, chiamate anche "ombre").

A seconda della direzione dei movimenti di mercato, le candele presentano una disposizione diversa dei prezzi di chiusura e apertura, oltre a colori differenti. Le candele ascendenti sono di solito rappresentate in verde o nero (riempite), mentre le candele discendenti sono di solito rosse o vuote (bianche).

Tra le molte varietà di grafici, il grafico a candele è probabilmente il più popolare tra trader e analisti. Forse perché i grafici a candele sono visivamente più facili da interpretare rispetto ai grafici a linee e a barre convenzionali.

Sin dalla sua creazione, i grafici a candele sono stati ampiamente utilizzati e studiati e sono ora una parte cruciale dei mercati finanziari. Pertanto, imparare a leggere le candele e a identificare i loro modelli è uno dei passaggi più basilari e vitali per qualsiasi aspirante trader.

Cantillon Effect

Acronimo di: Effetto Cantillon

Livello: intermedio

Argomento: economia

L'effetto Cantillon è un concetto economico che descrive come l'aumento della quantità di denaro in un'economia tende a beneficiare prima coloro che hanno accesso ai nuovi fondi (ad esempio, le banche centrali e i grandi istituti finanziari) rispetto a coloro che non ne hanno.

Questo effetto si verifica perché i primi a ricevere nuovi fondi possono utilizzarli per acquistare beni e attività prima che i prezzi aumentino, mentre coloro che ricevono i fondi più tardi vedono i prezzi aumentare senza beneficiare dello stesso aumento del potere d'acquisto.

L'Effetto Cantillon descrive l'effetto disomogeneo dell'inflazione sui beni e sugli asset di un'economia. Poiché la nuova moneta fiat viene immessa in un'economia in momenti specifici, i suoi effetti vengono percepiti da persone e industrie diverse in tempi diversi. Questo provoca una distorsione dei prezzi relativi e avvantaggia alcune parti mentre ne svantaggia altre.

Quando si aggiunge nuova moneta all'economia, aumenta naturalmente il prezzo di beni e attività. Tuttavia, non tutti i prezzi aumenteranno della stessa entità o nello stesso momento. L'Effetto Cantillon afferma che il primo destinatario della nuova offerta di moneta ha una opportunità di arbitraggio nel poter spendere il denaro prima che i prezzi siano aumentati.

Ciò è in parte dovuto al fatto che la nuova moneta fiat viene creata a costo quasi zero e data a soggetti specifici, di solito le banche. Queste banche hanno l'opportunità di spendere questo denaro in beni e attività il cui prezzo non ha ancora riflesso l'aumento dell'offerta di moneta. Le banche possono così acquistare beni a un tasso scontato.

Man mano che il nuovo denaro fluisce dalle banche centrali alle banche private, dagli investitori ai comuni cittadini, i prezzi iniziano gradualmente a riflettere l'aumento dell'offerta di moneta. Quando i cittadini comuni sperimenteranno l'aumento della massa monetaria, acquisteranno beni a prezzi più alti.

Pertanto, il flusso di nuova moneta attraverso l'economia è vantaggioso per le parti che ricevono i fondi per prime, e meno vantaggioso per quelle che li ricevono successivamente. Gli individui e le istituzioni più vicine alla banca centrale - banche e proprietari di asset - ottengono vantaggi finanziari a scapito di quelli meno collegati al sistema finanziario.

Come risultato dell'Effetto Cantillon, l'inflazione può essere vista come una tassa non legislativa e regressiva sul potere d'acquisto dei cittadini da parte del governo.

L'effetto Cantillon è stato originariamente descritto dall'economista belga Richard Cantillon nel XVIII secolo.

Cashu

Livello: avanzato

Argomento: tecnologia

Cashu è un sistema Chaumian chash gratuito e open source creato per Bitcoin.

Cashu offre una privacy quasi perfetta per gli utenti di applicazioni Bitcoin di custodia. Nessuno ha bisogno di sapere chi sei, quanti fondi hai e con chi effettui transazioni.

Cashu è protocollo ecash per applicazioni custodial Bitcoin strettamente integrato nella rete Lightning. Un sistema Ecash è composto da due parti, il mint e il wallet ecash. Le transazioni Ecash non sono tracciabili, sono istantanee e non richiedono commissioni.
Cashu è costruito per Bitcoin. I wallet utilizzano il nodo Lightning del mint per effettuare o ricevere pagamenti Bitcoin in cambio di ecash. Un mint Cashu non sa chi sei, qual è il tuo saldo o con chi stai effettuando transazioni. Gli utenti di un mint possono scambiare ecash privatamente senza che nessuno possa sapere chi sono le parti coinvolte.
I pagamenti Bitcoin vengono eseguiti senza che nessuno possa censurare utenti specifici.

CASP

Acronimo di: Crypto-asset Service Provider

Fornitori di servizi di Crypto Asset

Livello: avanzato

Argomento: politica

I CASP o CSP sono definiti dal MiCA come fornitori di servizi di cripto-asset.

Per servizio di cripto-asset si intende uno qualsiasi dei servizi e attività elencati di seguito relativi a qualsiasi cripto-asset:

- la custodia e l'amministrazione di cripto-asset per conto di terzi
- la gestione di una piattaforma di trading di cripto-asset
- lo scambio di cripto-asset con valuta fiat che ha corso legale
- lo scambio di cripto-asset con altri cripto-asset
- l'esecuzione di ordini di cripto-asset per conto di terzi
- il collocamento di cripto-asset
- ricezione e trasmissione di ordini di cripto-asset per conto di terzi
- fornire consulenza sui cripto-asset

Un CASP è definito dalla MiCA come qualsiasi persona la cui occupazione o attività è la fornitura di uno o più servizi di cripto-asset a terzi su base professionale.

Il termine CASP viene usato spesso come sinonimo di VASP o fornitore di servizi di asset virtuali, anche se la definizione che il MiCA da di CASP è più ampia

e include delle fattispecie che non rientrano nella definizione di VASP fatta dal FAFT/GAFI.

La definizione di CASP è più ampia di quella di VASP del FATF al fine di garantire che MiCA si applichi alla maggior parte delle società di criptovalute e per garantire che si possa in futuro applicare a nicchie di mercato che ancora non esistono.

CBDC

Acronimo di: Central Bank Digital Currency

Livello: intermedio

Argomento: legale

Le CBDC sono delle monete digitali che verrebbero emesse dalle banche centrali, con l'uso di tecnologie ispirate dalle criptovalute, ma che minano alla base i principi di base delle criptovalute e dei bitcoin.

Darebbero al governo un controllo e una supervisione totali sulle proprietà e sulle transazioni di ogni persona. In un'ironica inversione degli obiettivi fondamentali del Bitcoin come valuta anti-inflazionistica, decentralizzata e libera dalla mediazione di terzi, le CBDC cercano di appropriarsi dell'interesse per il Bitcoin e di principi come la sicurezza e la decentralizzazione che sono diventati sinonimo di Bitcoin, ma in realtà rappresentano l'antitesi.

Le CBDC sono una forma di valuta altamente centralizzata, priva delle proprietà anti-inflazionistiche del Bitcoin, in quanto il governo potrebbe coniare continuamente altri esemplari della valuta digitale proprio come fa con la valuta fiat, svalutandola costantemente.

Accentrando le informazioni e le disponibilità finanziarie dei cittadini in un database digitale controllato dal governo, le CBDC creerebbero uno stato di sorveglianza autoritario e costituirebbero un grave eccesso di potere governativo. Attraverso le CBDC, il governo diventerebbe sia stampatore di denaro che banca, distruggendo quei pochi controlli e bilanciamento del potere del governo ancora esistente di controllo sulle disponibilità finanziarie dei cittadini.

Concedendo al governo la proprietà della tecnologia di base del denaro, le CBDC permettono al governo di avere una totale discrezione su come e se i cittadini possono usare il loro denaro.

Le CBDC sono state accolte dal governo cinese, e sono in fase di studio e possibile implementazione da parte del governo europeo.

Anche la Russia sta attualmente sviluppando una propria valuta digitale, il cripto rublo, che, contrariamente al suo nome, sarà emesso dal governo senza alcuna attività di mining.

La posizione degli Stati Uniti, con l'amministrazione Trump, è assolutamente contraria: il 23 gennaio 2025 Trump ha firmato un ordine esecutivo volto a bloccare le CBDC (valute digitali delle banche centrali) e a favorire lo sviluppo di attività digitali, della tecnologia blockchain e di tecnologie correlate.

Nel dettaglio, l'ordine stabilisce che:

- Alle agenzie governative è vietato intraprendere qualsiasi azione per istituire, emettere o promuovere CBDC all'interno della giurisdizione degli Stati Uniti o all'estero. Inoltre, tutti i piani o le iniziative in corso presso qualsiasi agenzia, relativi alla creazione di una CBDC negli Stati Uniti, devono essere immediatamente interrotti, e non sarà consentito intraprendere ulteriori azioni per sviluppare o implementare tali piani o iniziative.
- Si supporta la crescita e l'uso responsabile di asset digitali, della tecnologia blockchain e di tecnologie correlate in tutti i settori dell'economia. L'ordine promuove e protegge la capacità di singoli cittadini e aziende private di accedere e utilizzare reti blockchain pubbliche aperte per scopi legittimi, senza il rischio di persecuzioni.
  Ciò include:
- – La possibilità di sviluppare e distribuire software.
- – La partecipazione alle attività di mining e validazione.
- – L'effettuazione di transazioni con altre persone senza censure illegali.
- – La gestione autonoma degli asset digitali tramite autocustodia.

centralized

centralizzato

Livello: base

Argomento: tecnologia

Un sistema centralizzato è un'architettura nella quale esiste una entità centrale che gestisce o controlla le risorse, i dati e le decisioni.

Bitcoin si caratterizza per il fatto di non essere un sistema centralizzato.

Spesso quando si confrontano sistemi o reti in relazione alla loro centralizzazione, viene fatto riferimento ai modelli descritti da Paul Baran che li distingue in:

- centralizzati,
- decentralizzati,
- e distributi.

I suoi modelli sono stati fondamentali per lo sviluppo di Internet e ha influenzato notevolmente l'architettura delle reti di comunicazione moderne.

CEX

Acronimo di: Centralized Exchanges

Exchange centralizzati

Livello: intermedio

Argomento: finanza

Gli Exchange centralizzati (CEX) sono un tipo di exchange di criptovalute gestito da una società che lo possiede in modo centralizzato. Gli Exchange centralizzati facilitano gli scambi tra gli utenti mantenendo un order book: la lista degli ordini di acquisto e vendita inviati da singoli trader. Gli ordini sono richieste di acquisto o vendita di un determinato importo di una specifica criptovaluta a un determinato prezzo. I CEX aggregano gli ordini dei loro utenti e quindi utilizzano un software per abbinare ed eseguire gli ordini di acquisto e vendita corrispondenti. Gli utenti CEX in realtà non si scambiano criptovalute o valute fiat, ma vengono solo aggiornati i loro conti. Quando gli utenti depositano i loro fondi fiat o cripto su un exchange, quest'ultimo assume la custodia di tali beni ed emette un importo corrispondente di IOU al trader. Lo scambio tiene traccia degli IOU di ogni utente internamente mentre cambiano di mano negli scambi e li converte in valuta reale solo al momento del prelievo dei fondi.

CFTC

Acronimo di: Commodity Futures Trading Commission

Livello: intermedio

Argomento: politica

Il principale regolatore statunitense per i derivati. L'agenzia ha stabilito che, in termini legali, le valute virtuali come Bitcoin sono commodity . Ciò significa che ha giurisdizione per supervisionare i derivati che utilizzano una valuta digitale e potenzialmente comminare sanzioni in caso di frode o manipolazione di tali derivati.

Chain

catena

Livello: base

Argomento: tecnologia

Abbreviazione di blockchain

Chain Analysis

Livello: intermedio

Argomento: legale

La block chain Bitcoin non contiene informazioni personali sugli utenti e sulle transazioni, ma informazioni pseudonime, ad esempio l'indirizzo del wallet è un codice numerico che nulla dice sull'utente se non le transazioni ad esso associate.

Inoltre ogni utente può generare quanti indirizzi vuole per le proprie transazioni. Per questo spesso si parla di anonimato per le criptovalute, anche se le informazioni più che anonime possono essere definite pseudonime.

La Chain analysis è una operazione di analisi delle transazioni sulla blockchain e altre informazioni recuperate esternamente per poter identificare gli utenti e tracciare le loro transazioni.

La Chain analysis è ampiamente utilizzata per market intelligence, l'analisi delle tendenze e le investigazioni, tra molte aree emergenti. L'obiettivo principale della Chain analysis è l'attribuzione: collegare asset quali bitcoin e eventi specifici a entità particolari o addirittura a individui.

L'attribuzione della proprietà, tuttavia, è spesso sfumata perché gli osservatori esterni possono solo dedurla in base a fattori come la disponibilità e la qualità delle prove. Le prove significano la dimostrazione che effettivamente un indirizzo appartiene a un individuo o a un'entità. A meno che tu stesso non sia il proprietario di un indirizzo, è molto difficile affermare con certezza assoluta a chi appartiene un indirizzo. Ecco perché anche gli stessi operatori del settore consigliano di considerare la Chain analysis più un'arte che una scienza.

Esistono diverse aziende che forniscono servizi di deanonimizzazione e altre analisi utilizzate da istituti finanziari, governi e le loro agenzie che con l'obbiettivo di prevenire frodi, riciclaggio di denaro e altre attività.

Ma è molto alto il rischio di uso e abuso di questi metodi e le possibilità di questi sistemi sono spesso sovra stimati, poiché non forniscono prove scientifiche, ma solo probabilità e il loro uso può portare a restrizioni ingiustificate sugli account quando vengono utilizzati per la conformità e, nel peggiore dei casi, per portare individui ignari nel radar delle forze dell'ordine senza una causa plausibile.

Attraverso la Chain Analysis si cerca anche di individuare transazioni potenzialmente illegali o illecite. Consiste nell'analizzare i dati presenti sulla blockchain, come gli indirizzi bitcoin, le transazioni e i flussi di fondi, allo scopo di ricostruire la cronologia degli scambi e identificare eventuali attività sospette.

Gli strumenti di Chain Analysis permettono di visualizzare in modo semplice e intuitivo i dati presenti sulla blockchain, in modo da individuare facilmente indirizzi e transazioni sospette. Inoltre, questi strumenti possono essere utilizzati per collegare indirizzi bitcoin a identità reali, rendendo possibile l'identificazione degli individui che utilizzano la criptovaluta per attività illecite.

La Chain Analysis è utilizzata sia dalle autorità di regolamentazione e dalle forze dell'ordine per indagare su attività illegali come il riciclaggio di denaro, il finanziamento del terrorismo e la frode, che da alcune società di servizi cripto

e le banche utilizzano queste tecniche per adempiere alle proprie responsabilità di conformità normativa e prevenire la criminalità finanziaria.

Le euristiche sono utilizzate nella Chain Analysis per identificare transazioni potenzialmente illegali o illecite all'interno della blockchain di Bitcoin. Le euristiche sono regole generali o algoritmi di base utilizzati per semplificare la ricerca e la classificazione dei dati.

In particolare, le euristiche vengono utilizzate per identificare pattern e tendenze nelle transazioni sulla blockchain, che possono indicare attività sospette. Ad esempio, un'euristica comune è quella di cercare transazioni che coinvolgono indirizzi noti per essere associati a attività illegali, come quelli presenti in liste nere.

Altri esempi di euristiche utilizzate nella Chain Analysis sono:

- Individuazione di transazioni che utilizzano molti indirizzi intermedi per nascondere la fonte dei fondi;
- Identificazione di cluster di indirizzi che sembrano appartenere alla stessa entità o persona;
- Individuazione di transazioni che presentano importi elevati o anomali;
- Ricostruzione della cronologia degli scambi tra indirizzi per identificare flussi di fondi sospetti.

chain split

Livello: intermedio

Argomento: tecnologia

Una chain split, o divisione della catena, si riferisce a un fork di una criptovaluta che a partire da uno specifico blocco della blockchain si divide in due rami separati che proseguono la catena in modo indipendente.

Tale split viene generalmente causato dalle modifiche sulle regole di consenso, che fa in modo che transazioni valide su un ramo della catena non lo siano nell'altro ramo.

Le ragioni di un chain split di criptovaluta sono molteplici. Con l'evoluzione dello spazio blockchain, gli sviluppatori di progetti di criptovalute hanno idee diverse su come e quale approccio adottare per l'ulteriore sviluppo della blockchain. Per questo motivo, spesso si verificano disaccordi ideologici tra gli sviluppatori di un progetto di criptovaluta che portano alla divisione della catena.

Ad esempio, Bitcoin Cash (BCH) è uno split della catena Bitcoin a partire dal blocco 478559 effettuato il 1° agosto 2017 a causa di una differenza di idee alternative sulla scalabilità, e poi dalla chain di Bitcoin Cash a novembre 2018 viene fatto un ulteriore chain split con la creazione di Bitcoin SV.

Una chain split si verifica quando gli sviluppatori costruiscono una moneta indipendente basata sul codice di una blockchain consolidata, portando a una

separazione, o split, dal progetto madre originale.

Ecco alcuni esempi di hard fork Bitcoin che hanno generato una chain split:

- Bitcoin Cash (BCH): creato nel 2017 per aumentare la dimensione dei blocchi
- Bitcoin SV (BSV): creato nel 2018 per aumentare ulteriormente la dimensione dei blocchi
- Bitcoin Gold (BTG): creato nel 2017 per rendere più decentralizzato il mining
- Bitcoin Diamond (BCD): creato nel 2017 per migliorare la scalabilità

Uno dei rischi quando si crea una chain split, è la vulnerabilità ai Replay Attack.

ChainWork

Livello: intermedio

Argomento: tecnologia

Il ChainWork è il valore utilizzato dalla rete Bitcoin, in caso di blockchain composte da diversi blocchi in conflitto tra loro, per stabilire il consenso su quale sia la catena più lunga, o Longest chain, da considerarsi come valida.

Inizialmente Satoshi aveva stabilito il consenso sulla catena con il maggior numero di blocchi validi come metrica per determinare la catena più lunga. Però scegliere la catena semplicemente contando i blocchi consente alcuni attacchi estremamente facili da effettuare, e nel 2010 è stato introdotto il calcolo del ChainWork per determinare la catena più lunga.

Il ChainWork è uguale alla somma del BlockWork dei suoi blocchi. Il BlockWork è il numero medio di hash che si prevede siano necessari da calcolare per generare un blocco data una certa difficulty (quindi è diverso dalla difficulty ma dipende da questa). Siccome la difficulty viene regolata ogni 2016 blocchi (circa ogni 2 settimane), i blocchi minati nell'intervallo di tempo nel quale c'è la stessa difficoltà hanno lo stesso BlockWork. Il termine BlockWork è poi stato sostituito con BlockProof.

Change Output

Output di resto

Livello: avanzato

Argomento: tecnologia

In Bitcoin, un Change output, o output di resto, è un output che viene creato come resto in una transazione.

Bitcoin non utilizza conti e saldi. Vengono utilizzati gli UTXO, o output non spesi delle transazioni.

Questi possono essere paragonati a banconote fisiche in quanto, quando vengono spesi, di solito è necessario dare il resto in quanto il loro importo non corrisponde quasi mai a quello pagato.

Quando un utente effettua una transazione, utilizza uno o più input di sua proprietà per generare l'output desiderato. Tuttavia, poiché la quantità di Bitcoin trasferita in una transazione deve esattamente corrispondere alla somma degli input, può verificarsi che la somma degli input in ingresso sia maggiore dell'importo effettivamente necessario.

Un'output sarà inviato all'indirizzo del destinatario e l'altro output sarà restituito al wallet del mittente, di solito tramite un indirizzo diverso, in un output chiamato Change output.

L'importo di questo secondo output sarà il resto, che corrisponderà alla somma degli ingressi meno l'importo speso nel primo output e la fee di transazione.

Ad esempio, se un utente ha un input di 2 BTC e vuole inviare solo 0.5 BTC e imposta come fee 0.000001, il change output sarà 1,499999 BTC, che viene restituito all'utente come resto. Questi change output sono in genere inviati a un nuovo indirizzo generato dal proprio portafoglio per evitare di condividere informazioni sull'indirizzo di origine.

Queste considerazioni possono essere considerate come euristiche per la Chain Analysis, in particolare la Round Amounts Heuristic: l'output con un importo arrotondato è del destinatario del pagamento, e quindi l'altro output anche se inviato ad un nuovo indirizzo si può presumere appartenga al mittente.

Channel jamming

Livello: avanzato

Argomento: tecnologia

Il channel jamming è un tipo di attacco su Lightning Network che si verifica quando un'entità malintenzionata, effettuando un pagamento a se stessa tramite canali di terze parti ne blocca la liquidità non rivelando mai il preimage, in modo tale che il pagamento non venga mai completato.

Lightning Network è una rete di nodi che si aiutano (di solito a pagamento) a vicenda per effettuare pagamenti tramite canali di pagamento: se Alice e Bob non hanno un canale diretto, possono utilizzare un percorso composto da più nodi di instradamento tra di loro, multi-hop, per inoltrare questo pagamento regolando i balance nei canali lungo il percorso. È importante che questi pagamenti multi-hop siano atomici, AMP Atomic Multipath Payment o Pagamenti Multipercorso Atomici, ovvero devono tutti andare a buon fine e nel caso anche uno solo fallisca devono fallire tutti, altrimenti c'è il rischio che i nodi di instradamento prendano i fondi senza inoltrarli.

I pagamenti multi-hop avvengono in due fasi:

- bloccando i fondi sul percorso dal mittente al destinatario
- e poi spostando i saldi propagando il preimage dal destinatario al mittente.

L'idea principale alla base del jamming è occupare le capacità di instradare i nodi per inoltrare i pagamenti effettuando pagamenti falsi e non completandoli mai. Per la durata dell'attacco, diventa impossibile per i nodi di instradamento inoltrare altri pagamenti (onesti).

Per bloccare determinati canali, un utente malintenzionato finge di effettuare un pagamento a se stesso tramite quei canali e non rilascia mai il preimage dal lato del destinatario.

Esistono due tipi di jamming:

- **amount jamming**, per il quale un attaccante blocca una porzione significativa della capacità del canale target
- **slot jamming**, per il quale un attaccante blocca le capacità di inoltro del canale target esaurendo il limite dei pagamenti in-flight

Gli attacchi di channel jamming sono attacchi DoS Denial of Service in cui un attaccante può impedire a una serie di canali distanti fino a 20 hop di utilizzare parte o tutti i loro fondi per un periodo di tempo prolungato.

Un nodo LN può instradare un pagamento verso se stesso attraverso un percorso di 20 o più hop. Questo crea due possibili vie per gli attacchi di channel jamming:

- L'attacco **Liquidity jamming** (originariamente chiamato loop attack nel 2015) consiste nel fatto che un attaccante con una quantità di denaro pari a x (ad esempio 1 BTC) la invia a se stesso attraverso altri 20 canali, ma ritarda a saldare o a rifiutare il pagamento, bloccando temporaneamente un totale di 20x fondi appartenenti ad altri utenti (ad esempio 20 BTC). Dopo diverse ore di blocco del denaro di altri utenti, l'aggressore può annullare il pagamento e ricevere un rimborso completo delle spese sostenute, rendendo l'attacco essenzialmente gratuito.
- L'attacco **HTLC jamming** consiste nell'invio da parte di un aggressore di 483 piccoli pagamenti HTLC attraverso una serie di 20 canali: un canale Lightning può avere solo 483 HTLC in attesa in ogni direzione che può instradare, questo perché esiste un limite massimo di dimensione di quanto può essere grande una transazione Bitcoin. Se si aggiungono più di 483 HTLC per direzione nel canale, la transazione per chiudere il canale, se necessario, sarebbe troppo grande e non valida da inviare alla rete. Ciò renderebbe tutto ciò che è presente nel canale inapplicabile on-chain. In questo caso, un attaccante con due canali, ciascuno con 483 slot, può bloccare oltre 10.000 slot HTLC onesti, sempre senza pagare alcuna fee.

Quindi, un attaccante può cercare di bloccare tutta la liquidità di un canale o di bloccare tutti gli slot HTLC di un canale. Entrambe le strategie renderebbero il canale inutilizzabile, ma il blocco degli slot è generalmente più economico del blocco della quantità. L'attaccante deve disporre di monete sulla rete per eseguire questo attacco, quindi instradare il valore minimo consentito per un

HTCL con capacità di 483 sarà più conveniente che cercare di bloccare tutta la liquidità disponibile nel canale.

Ci sono molte ragioni per eseguire questo attacco. In primo luogo, un'entità malintenzionata che volesse attaccare Bitcoin stesso potrebbe bloccare tutti i canali chiave nel "cuore" della rete, in modo da rendere la maggior parte della rete inutilizzabile per l'instradamento dei pagamenti, fatta eccezione per i nodi che sono molto strettamente connessi tra loro. Ciò richiederebbe un numero di monete molto più elevato per raggiungere questa scala, ma non è un'eventualità da scartare quanto più il Bitcoin cresce e diventa un'alternativa al denaro e ai sistemi di pagamento approvati dai governi.

In secondo luogo, un nodo di routing, o un commerciante, potrebbe tentare di eseguire l'attacco a un concorrente per spingere le commissioni verso di lui rispetto alla concorrenza. Un commerciante che vende prodotti simili potrebbe intasare i canali di un concorrente per impedire ai clienti di fare acquisti lì, nella speranza di incentivarli a comprare nel suo negozio. Un nodo di routing che ha una connettività di canali simile a quella di un altro nodo potrebbe bloccare i canali del nodo di routing concorrente per renderli inutilizzabili per l'instradamento dei pagamenti. Con il tempo questo distruggerebbe la reputazione del nodo in termini di affidabilità del routing e, a causa della connettività simile, renderebbe sempre più probabile che i portafogli degli utenti scelgano il nodo dell'attaccante per instradare i pagamenti attraverso la rete.

Questi attacchi possono essere ancora più efficienti dal punto di vista del capitale per l'aggressore, se si instradano circolarmente attraverso un singolo canale più volte. Se sono abbastanza vicini alla vittima sulla rete, possono costruire un percorso di pagamento che si aggira e continua a passare attraverso il canale della vittima. Ci sono dei limiti alla lunghezza di un percorso di pagamento, quindi non si può fare all'infinito, ma un percorso di pagamento ad anello come questo può ridurre drasticamente la quantità di monete di cui l'attaccante ha bisogno per bloccare completamente il canale della vittima.

Questo tipo di attacco può essere particolarmente dannoso per la rete Lightning Network poiché può causare la chiusura di molti canali di pagamento, riducendo così la capacità della rete di gestire le transazioni. Esistono diversi modi per proteggere la rete dal channel jamming, come ad esempio l'utilizzo di tecniche di routing basate sulla reputazione o la creazione di canali di pagamento con una capacità maggiore.

Circulating supply

Disponibilità circolante

Livello: intermedio

Argomento: economia

La Circulating supply, in italiano Disponibilità circolante o Offerta circolante,

è il totale delle monete in circolazione di una specifica criptovaluta nel mercato e nelle mani del pubblico in generale.
Il termine offerta circolante si riferisce al numero di monete o token di criptovaluta che sono pubblicamente disponibili e circolano sul mercato.
L'offerta circolante di una criptovaluta può aumentare o diminuire nel tempo.

Nel caso dei bitcoin, l'offerta circolante di Bitcoin aumenta gradualmente e all'inizio di aprile 2022 l'offerta circolante bitcoin ha raggiunto i 19 milioni di bitcoin totali minati, e raggiungerà l'offerta massima, Max supply, di 21 milioni di monete presumibilmente intorno al 2140.
Tale aumento graduale è legato al processo di mining che genera nuove monete, la Block Subsidy, all'interno del nuovo blocco che viene minato in media ogni 10 minuti.
Su alcune cripto, eventi di coin burn causano una diminuzione dell'offerta circolante, rimuovendo definitivamente le monete dal mercato, ad esempio sulla blockchain Ethereum a seguito dell'implementazione dell'EIP-1559.
L'offerta circolante si riferisce alle monete che sono accessibili al pubblico e non deve essere confusa con l'offerta totale o l'offerta massima. L'offerta totale è usata per quantificare il numero di monete esistenti, cioè il numero di monete già emesse meno le monete bruciate. L'offerta totale è fondamentalmente la somma dell'offerta circolante e delle monete che sono bloccate in deposito. D'altra parte, l'offerta massima quantifica la quantità massima di monete che esisterà mai, comprese le monete che saranno estratte o rese disponibili in futuro.
Inoltre, l'offerta circolante di una criptovaluta può essere utilizzata per calcolare la sua capitalizzazione di mercato, che viene generata moltiplicando il prezzo corrente di mercato per il numero di monete in circolazione. Quindi, se una certa criptovaluta ha un'offerta circolante di 1.000.000 di monete, che vengono scambiate a $5,00 ciascuna, la capitalizzazione di mercato sarebbe pari a $5.000.000.

CISA

Acronimo di: Cross-Input Signature Aggregation

Aggregazione di firme tra input incrociati

Livello: avanzato

Argomento: tecnologia

L'idea alla base di Cross-Input Signature Aggregation, ovvero aggregazione delle firme, è di fornire una sola firma per transazione Bitcoin anche quando ci sono più input.
CiSA rappresenta un potenziale soft fork di Bitcoin che riduce il peso delle transazioni.

Un vantaggio chiave dell'algoritmo di firma di Schnorr rispetto a ECDSA è la sua linearità. Questa caratteristica consente a più firmatari di creare un'unica

firma che possa facilmente verificare l'autorizzazione di un messaggio tramite più chiavi.

Le firme Schnorr consentono di rappresentare transazioni con più input, ciascuno con una firma diversa, attraverso un'unica firma digitale. Questa funzionalità può contribuire a risparmiare fino al 30% dello spazio nei blocchi Bitcoin, aumentando quindi la scalabilità della rete consentendo di avere maggiori transazioni in ogni blocco. Inoltre, questo sistema migliora notevolmente la privacy, poiché non è possibile tracciare le firme con le voci corrispondenti all'interno di ogni transazione utilizzando una singola firma.

Attualmente per garantire la privacy nelle transazioni è possibile utilizzare Coinjoin, tuttavia questo metodo non offre una buona user experience all'utente, richiede tempo e denaro, e non tutti hanno le conoscenze tecniche per effettuare coinjoin, il che scoraggia molte persone dal farlo. Inoltre, più input richiedono più firme.

Con CiSA, se Alice vuole pagare Bob e Carol vuole pagare Dave, i paganti Alice e Carol possono combinare le rispettive transazioni creando un'unica firma che dimostra che tutti i proprietari delle chiavi hanno collaborato alla creazione della firma.

Le firme sono la parte più grande di una transazione, quindi ridurre le firme significa che la transazione diventa più piccola. Ciò si traduce in un maggior numero di transazioni per blocco e in una riduzione delle commissioni per transazione.
Una transazione con un solo input avrà lo stesso costo, mentre una transazione con 2 input avrà un significativo risparmio, e una transazione con più input avrà un risparmio ancora maggiore in base al numero di input. Anche se ci sono centinaia di input, è richiesta solo una firma, rendendo le transazioni più convenienti in base al numero di input. Ciò consentirà di risparmiare circa 16 vbyte per ogni keypath spend dopo il primo input, con un risparmio significativo per il consolidamento e le coinjoin.

Questo potrebbe persino rendere la spesa basata su coinjoin più economica di quella effettuata in modo isolato, incentivando l'utilizzo di questa forma di spesa con maggiore privacy.

Clearnet

Livello: intermedio

Argomento: tecnologia

Clearnet è il termine usato in contrapposizione a Darknet, che in genere descrive i servizi costruiti su Tor o altre reti di anonimato, la cui connessione è criptata e anonimizzata.

In genere si riferisce all'Internet pubblicamente accessibile. A volte Clearnet è usato come sinonimo di "surface web", escludendo sia la Darknet che il Deep

Web. Il World Wide Web è uno dei servizi distribuiti più popolari su Internet e il surface web è composto dalle pagine web e dai database indicizzati dai motori di ricerca tradizionali.

Poiché la Darknet non è accessibile al pubblico, potrebbe essere intesa come parte del Deep Web. Il Deep Web, che non è indicizzato, è comunque pubblicamente accessibile. Comprende portali web di banche dati che richiedono ricerche testuali e siti web interattivi che richiedono all'utente un input maggiore rispetto al semplice clic sui collegamenti ipertestuali.

Client

Livello: intermedio

Argomento: tecnologia

In informatica, un client è un componente hardware o software che accede a un servizio reso disponibile da un server, secondo il modello client-server.

Nel caso di Bitcoin e delle criptovalute, un client è il software per l'utente finale che facilita la generazione e la sicurezza di chiavi private, l'invio di pagamenti per conto di una chiave privata e fornisce opzionalmente: informazioni utili sullo stato della rete e sulle transazioni; informazioni relative alle chiavi private sotto la sua gestione; syndication (dall'inglese "sindacazione", "consorzio") di eventi di rete ad altri client peer.

Il wallet per criptovalute può essere considerato un client, e in particolare viene definito lightweight client quando non ha una sua copia della blockchain e si deve collegare ad un full node .

closing transaction

Livello: avanzato

Argomento: tecnologia

La Closing Transaction su Lightning Network è la transazione di chiusura di un canale.

Quando si utilizza Lightning Network per effettuare transazioni, i fondi non vengono immediatamente inviati sulla blockchain principale, ma vengono invece gestiti attraverso un canale di pagamento bidirezionale tra due parti.

Una volta che entrambe le parti decidono di chiudere il canale di pagamento, viene creata una "Closing Transaction" per spostare i fondi rimanenti nel canale sulla blockchain.
Questa transazione di chiusura può essere creata in modo collaborativo dalle due parti o, in caso di disaccordo, una parte può forzare unilateralmente la chiusura del canale attraverso una force close o chisura forzata.

In ogni caso, la Closing Transaction è un'operazione critica per chiudere il canale e permettere alle parti di accedere ai fondi che vi sono stati bloccati durante l'utilizzo di Lightning Network.

Se entrambi i partner di canale concordano di chiudere un canale, creeranno una Closing Transaction che riflette la commitment transaction più recente.
Dopo lo scambio di firme per una Closing Transaction, non devono essere effettuati ulteriori aggiornamenti del canale.

La chiusura reciproca di un canale con l'aiuto di una Closing Transaction ha il vantaggio di richiedere un minor numero di transazioni blockchain per rivendicare tutti i fondi, rispetto all'imposizione unilaterale della chiusura di un canale tramite la pubblicazione di una commitment transaction. Inoltre, i fondi per entrambe le parti sono immediatamente spendibili da una Closing Transaction.

Cloud Mining

Livello: intermedio

Argomento: tecnologia

E un tipo di mining effettuato utilizzando un data center remoto con potenza di elaborazione condivisa.
Il cloud mining consente agli utenti di estrarre Bitcoin o criptovalute alternative senza gestire l'hardware. Le piattaforme di mining sono alloggiate e mantenute in una struttura di proprietà della società mining e il cliente deve semplicemente registrare ed acquistare contratti o azioni di mining. Poiché il cloud mining viene fornito come servizio, generalmente c'è un costo e questo può comportare rendimenti inferiori per il miner.

CLTV

Acronimo di: Check Lock Time Verify

Livello: avanzato

Argomento: tecnologia

CLTV è un'interessante funzionalità di timelock che esiste in Bitcoin progettata per consentire ai suoi script di eseguire pianificazioni temporali avanzate sulle transazioni. CLTV rende possibile bloccare output (UTXO) che non possono essere spesi fino a quando non è arrivato un tempo determinato in precedenza.

CLTV è stato introdotto a dicembre 2015 nel soft fork definito dal BIP-0065, nel quale lo sviluppatore Peter Todd descrive il nuovo Opcode OP_CHECKLOCKTIMEVERIFY. Questa funzione consente a una transazione Bitcoin di rimanere bloccata nel tempo e non diventare effettiva fino al raggiungimento di una data e ora o uno specifico block height.

CLTV può essere utile per casi nei quali si vuole pianificare pagamenti futuri per date specifiche.

Come funziona CLTV Quando un utente stabilisce ed esegue una transazione con il codice OP_CHECKLOCKTIMEVERIFY, gli output di questa transazione saranno attivati solo quando la condizione stabilita sarà soddisfatta e non quando la transazione sarà eseguita. Ciò significa che la transazione viene eseguita correttamente ma le criptovalute rimarranno bloccate nel tempo fino a un momento futuro.

Il codice OP_CHECKLOCKTIMEVERIFY viene eseguito come parte di uno script Bitcoin e la sua programmazione si basa sull'uso di Unix Timestamp o su blockheight all'interno della blockchain.

Le condizioni per il fallimento dello script in una transazione CLTV sono le seguenti:

1. che lo stack sia vuoto e che non vi sia un tempo definito per il codice da eseguire il confronto e la verifica.
2. che l'elemento superiore dello stack sia inferiore a quello della condizione stabilita per sbloccare gli output. Ciò indica che il tempo necessario per sbloccare la transazione non è trascorso.
3. Un'altra condizione di fallimento si verificherà se il timelock stabilito viene misurato in block height e l'elemento superiore dello stack utilizza misurazioni del tempo (in secondi) o viceversa.
4. il campo nSequence di questa voce è impostato su 0xFFFFFFFF.

Una transazione CLTV può essere inclusa nella blockchain solo una volta che ha superato il tempo o le condizioni stabilite. Una volta che ciò accade, le transazioni CLTV vengono immediatamente verificate e aggiunte alla blockchain e vengono considerate spese.

Relazione CLTV e nLockTime Sia CLTV che nLockTime sono due funzioni che consentono a Bitcoin di programmare azioni che dipendono dal tempo o dall'altezza del blocco per la loro corretta esecuzione. nLockTime garantisce che Bitcoin possa pianificare l'esecuzione delle transazioni a una certa block height o timestamp, mentre CLTV consente di aggiungere un ulteriore livello di verifica e programmazione a nLockTime. Questo perché CLTV prende nLockTime e verifica che sia presente un insieme aggregato di condizioni pianificate per la sua attivazione, una situazione che era molto più diretta con nLockTime originale. CLTV consente anche di alterare alcune condizioni originali della transazione se determinate condizioni sono soddisfatte.

Ad esempio, un indirizzo multi-firma 2 su 3, che non è stato mosso in un certo periodo di tempo, può modificare i suoi parametri di autenticazione in 1 su 3, in modo che alcune delle persone inizialmente autorizzate possano movimentare i fondi in esso contenuti. Questa è una funzionalità unica che CLTV può offrire che nLockTime da solo non può fare.

Una delle maggiori caratteristiche di CLTV è che il suo utilizzo consente

la creazione di script che possono facilmente modificare le condizioni per l'attivazione di un evento o transazione nella blockchain di Bitcoin.

Implementazione di CLTV Una delle potenzialità più grandi e più importanti della funzione CLTV è quella di consentire la creazione di canali di pagamento e che questi possano essere implementati correttamente. Attraverso i canali di pagamento è possibile creare micro-transazioni al di fuori della blockchain. Tutto questo senza dover pagare tante commissioni per ognuna e senza appesantire la blockchain.

Nei canali di pagamento, un utente può effettuare una transazione a un altro depositando una certa quantità di criptovalute in un file indirizzo multi-firma (MultiSig). Entrambi gli utenti avranno accesso a quell'indirizzo. E l'utente che esegue la transazione può firmare piccole transazioni che verranno fatte all'altro utente da quei fondi.

Coin

moneta

Livello: base

Argomento: tecnologia

Il termine coin, tradotto in moneta, viene utilizzato per indicare una criptovaluta o denaro digitale, e a volte per indicare un asset di criptovaluta per distinguerlo da un token.

Nei Bitcoin, quelle che chiamiamo "coin" o monete esistono solo per convenzione. Il protocollo non conosce la nostra nozione di monete. Conosce solo i sats e gli output (UTXO) delle transazioni spesi o non spesi. Gli output spesi sono input di transazioni passate. Se la somma di uno o più output raggiunge i 100 milioni di sats, lo chiamiamo "1 Bitcoin".

Naturalmente, è molto più facile parlare di "monete", "indirizzi" e "portafogli", perché conosciamo queste cose grazie alla nostra comune esperienza. Abbiamo una comprensione intuitiva di queste metafore, quindi è chiaro cosa succede se una "moneta" si sposta da un "portafoglio" a un altro "portafoglio" - o almeno così pensiamo.

Sebbene l'immagine mentale delle monete che si spostano da un portafoglio all'altro in modo intuitivo, facile da capire e sia confortante, tuttavia è sbagliata. Ciò che accade nella rete bitcoin è molto più interessante ed elegante rispetto alle monete d'oro che passano da un borsellino all'altro. Bitcoin è informazione, non un oggetto fisico e quindi non viene spostato in alcun senso fisico.

Coin selection

Livello: intermedio

Argomento: tecnologia

Con Coin Selection, in italiano letteralmente tradotto in selezione delle monete, si intende la scelta delle coin o UTXO come input in una transazione.

Il saldo del wallet, anche se visualizzato come importo unico, può essere diviso in diversi UTXO, analogamente a un portafoglio che contiene diverse banconote e monete.
Questo insieme di UTXO viene chiamato pool UTXO del wallet.

Quando si effettua una transazione, il wallet deve selezionare le monete necessarie dal pool UTXO.
La selezione degli UTXO può avvenire automaticamente o manualmente da parte dell'utente nei wallet che offrono questa funzione. In tal caso il termine Coin Selection è sinonimo di CoinControl.

Gli UTXO che vengono selezionati come input in una transazione vengono chiamati *input set*.

La maggior parte dei primi wallet Bitcoin implementava strategie di selezione delle monete relativamente semplici, come spendere gli UTXO nell'ordine in cui sono stati ricevuti (first-in, first-out). Tuttavia, poiché le commissioni sono diventate più significative, alcuni wallet hanno adottato algoritmi più avanzati per ridurre le dimensioni delle transazioni e pagare fee più basse.

Le strategie di selezione delle monete possono essere utilizzate anche per migliorare la privacy onchain cercando di evitare l'uso di UTXO associati a transazioni precedenti in transazioni successive non correlate.

Ci sono diverse strategie o algoritmi per la coin selection, tra cui:

- CoinGrinder
- Branch and Bound

La scelta di un algoritmo può influenzare le dimensioni della transazione, le relative commissioni e la frammentazione degli UTXO dopo la transazione.

Con fee basse e un wallet con UTXO frammentati, può essere utile selezionare il maggior numero di input di piccole dimensioni per consolidare le monete in una transazione, cosa che con fee alte risulterebbe antieconomica. Viceversa, con fee alte, è conveniente selezionare gli input più grandi necessari per raggiungere l'importo richiesto dalla transazione.

L'algoritmo CoinGrinder cerca l'input set con peso minimo.
Prima dell'introduzione di CoinGrinder, Bitcoin Core utilizzava un algoritmo di coin selection basato su un semplice ordinamento delle UTXO in base al loro valore. Questo algoritmo era semplice da implementare ma poco efficiente e poteva generare transazioni con commissioni elevate.

Dalla sua introduzione, CoinGrinder è diventato l'algoritmo di coin selection predefinito in Bitcoin Core ed è utilizzato dalla maggior parte dei wallet Bitcoin.

Il wallet Bitcoin Core ha il parametro *consolidatefeerate* che stabilisce la fee massima (in BTC/kvB, di default a 0,00001) alla quale la creazione delle transazioni può utilizzare più input di quelli strettamente necessari, in modo da ridurre il pool UTXO del wallet.

Dalla versione 27.0 di Bitcoin Core, CoinGrinder è attivo solo quando le fee sono considerate elevate (sulla base del parametro -consolidatefeerate predefinito: 30+sat/vB, basato sul parametro × 3).
L'algoritmo Branch And Bound verrà disabilitato quando viene utilizzata la funzione di sottrazione delle fee dagli output.

Coinbase

Livello: base

Argomento: economia

Nel contesto di Bitcoin e delle criptovalute, il termine coinbase è noto come:

- la transazione coinbase, meglio descritta in questo glossario nella apposita pagina coinbase transaction
- da non confondere con l'exchange americano Coinbase, una delle più grandi società che si occupa di Bitcoin

coinbase transaction

Livello: intermedio

Argomento: tecnologia

Una coinbase transaction, transazione coinbase, è la prima transazione che viene inserita in un blocco Bitcoin dai miner.

La coinbase transaction è fondamentale perché:

- È il meccanismo con cui vengono creati nuovi bitcoin
- Incentiva i miner a mantenere sicura la rete
- Definisce il tasso di inflazione controllato e prevedibile di Bitcoin

Attraverso la coinbase transaction, il miner riceve la ricompensa, o block reward, per il lavoro effettuato per validaresvolto nel validare il blocco e aggiungerlo alla block chain.

La block reward è composta da:

- – block subsidy: nuovi bitcoin generati dal nulla. Questo è l'unico modo in cui vengono generate nuove monete Bitcoin. La quantità di Bitcoin generata per ogni blocco diminuisce nel tempo, dimezzandosi circa ogni quattro anni (processo noto come halving).
- – fee: commissioni associate alle transazioni incluse nel blocco

I bitcoin di questa ricompensa vengono assegnati a uno o più output.

Un blocco può contenere una sola coinbase transaction.

La struttura della coinbase transaction è simile alle altre transazioni, con alcune eccezioni:

A differenza delle altre transazioni, una coinbase transaction non consuma UTXO come input. Quindi quello spazio che nelle transazioni normali viene chiamato scriptSig, viene considerato il *coinbase data*, in cui il miner può inserire informazioni arbitrarie, ad esempio il messaggio del miner, l'altezza del blocco o un "extra nonce" per il mining.
La prima Coinbase Transaction della storia, quella del Genesis Block, conteneva questo messaggio nella coinbase data: `The Times 03/Jan/2009 Chancellor on brink of second bailout for banks`

Gli output della coinbase possono essere spesi solo dopo la conferma di 100 blocchi. Se il blocco include transazioni SegWit, la transazione Coinbase deve includere un commit per gli identificatori delle transazioni dei witness in un'uscita aggiuntiva.

Indice precedente ffffffff (in esadecimale): in una transazione normale, l'indice specifica quale output della transazione precedente viene speso (es. 0 per il primo output).
Nella coinbase, questo campo viene impostato a ffffffff (valore massimo di un intero a 32 bit senza segno, pari a 4294967295), che è un indice non valido. Questo segnala che l'input non fa riferimento a nessun output esistente.

CoinControl

Livello: intermedio

Argomento: tecnologia

La CoinControl è una funzione presente in alcuni wallet Bitcoin che consente agli utenti di avere il controllo completo sulla scelta delle transazioni che vengono incluse nei loro pagamenti. In particolare, CoinControl consente di selezionare manualmente le singole transazioni in entrata, chiamate anche input o UTXO, che si desidera utilizzare per il pagamento. Questo può essere utile per diverse ragioni:

- Privacy: selezionando input specifici, è possibile evitare di far sapere a terzi quali indirizzi bitcoin si possiedono.
- Fee: selezionando input con fee basse, è possibile risparmiare denaro sulle fee di transazione.
- Controllo: in alcuni casi, può essere utile avere il controllo completo su quale coin si sta utilizzando per un determinato pagamento.

In generale, CoinControl può essere una funzione utile per gli utenti avanzati che desiderano avere il massimo controllo sui loro pagamenti Bitcoin. Tenere

presente che non tutti i wallet supportano CoinControl, quindi quindi bisogna verifica se questa funzionalità è disponibile nel proprio wallet se si ritiene utile utilizzarla.

A volte il termine Coin Control viene usato come sinonimo di Coin Selection, anche se Coin Selection può riferirsi anche al meccanismo utilizzato in automatico dal wallet per la scelta degli input della transazione.

Coinjoin

Livello: avanzato

Argomento: tecnologia

CoinJoin è una tecnica per rendere le transazioni più anonime e rendere più difficili le operazioni di chain analysis.

Una transazione CoinJoin mette insieme un grande numero di mittenti e destinatari in un'unica transazione con molti importi identici, in modo che un osservatore non possa determinare facilmente chi stia trasferendo un importo a chi.

CoinJoin è un protocollo trustless per mescolare UTXO di più proprietari, al fine di rendere difficile per le parti esterne utilizzare la cronologia delle transazioni della blockchain per determinare chi possiede quale moneta. Si tratta di creare in modo collaborativo una singola transazione che spende uno o più UTXO di ogni partecipante in nuovi indirizzi per ogni partecipante, rendendo più difficile tracciare la storia delle transazioni di ogni uscita.

CoinJoin nasce da una proposta del 2013 di Gregory Maxwell, e diverse implementazioni indipendenti hanno fornito supporto per varie forme di CoinJoin.

Le transazioni Bitcoin sono costituite da input e output. Quando fai una transazione, prendi i tuoi UTXO come input, specifichi gli output e poi firmi gli input. Un CoinJoin serve a "rompere" l'associazione tra le transazioni e lo fa attraverso una transazione con più partecipanti che vengono coordinati tra loro da un terzo (attraverso il software wallet).

Attraverso una operazione trustless vengono mischiati UTXO da più proprietari al fine di rendere difficile per le parti esterne l'utilizzo della cronologia delle transazioni della blockchain determinare chi possiede quale moneta.
Si dichiarano gli input e gli output che si desidera includere e vengono trasformati in una transazione unica che viene firmata da ogni partecipante prima di essere trasmessa alla rete.

In forma molto semplice: Alice, Bob e Carol forniscono ciascuno un UTXO da 1,1 BTC e generano un nuovo indirizzo dove vogliono ricevere i loro output. Alice crea una transazione che spende quei 3,3 BTC in 3 uscite da 1 BTC (e 0,3 BTC come commissione), una a ciascuno dei 3 indirizzi generati dai partecipanti. Alice, Bob e Carol dovranno tutti firmare la transazione, poiché solo loro possono

firmare per i propri input. Una volta che tutte le firme sono state aggiunte alla transazione, chiunque può trasmetterla e il CoinJoin è completa. In nessun momento i partecipanti hanno accesso alle monete degli altri.

CoinJoin è distinto dai Mixing Service in quanto gli operatori CoinJoin non prendono mai la custodia di alcun fondo. Gli utenti mantengono il controllo del loro bitcoin in ogni momento.

Una volta che i partecipanti hanno firmato, la transazione non può essere modificata senza diventare non valida e questo serve a evitare il rischio che chi coordina scappi con i fondi.

Immagina la transazione come un salvadanaio dove metti le coin che poi vengono mescolate, in modo che l'unico legame tra le vecchie e le nuove UTXO sia la transazione stessa. Alla fine ciò che si vede è che un partecipante ha fornito uno degli input ed è forse il nuovo proprietario di un output risultante.

Per costruire una transazione CoinJoin, gli utenti collaborano con gli input nella transazione e ricevono le stesse quantità di bitcoin degli output, il tutto in quantità uniformi. Ad esempio, se 5 utenti immettono importi di 1, 2, 3, 4 e 5 BTC, ci saranno cinque input per un totale di 15 BTC e ci saranno 15 output, ciascuno del valore di 1 BTC e diventa impossibile associare i destinatari degli importi da 1 BTC al mittente.

Sebbene sia possibile che un CoinJoin assomigli a un pagamento batch, può essere abbastanza facile da identificare onchain e alcuni exchange si sono rifiutati di accettare monete con una storia recente di CoinJoin e per questo motivo può essere più efficace coinswap per ottenere questo scopo.

Sebbene il processo sembri chiaro in teoria, in pratica unire le transazioni è difficile per diversi motivi. Affinché i partecipanti al join rimangano anonimi, dovrebbero connettersi attraverso una rete Tor, devono conoscere un po' di codice e devono fidarsi l'uno dell'altro.

Per superare questi ostacoli, gli sviluppatori di soluzioni CoinJoin hanno iniziato presto a creare strumenti che rendessero il processo automatico per la maggior parte degli utenti. I primi tentativi di creare uno strumento CoinJoin sono stati incorporati nei wallet. I primi esempi sono stati Dark Wallet, JoinMarket e SharedCoins. Queste piattaforme miravano a fornire un ulteriore livello di mascheramento dei dati per gli utenti che effettuavano transazioni in Bitcoin.

Il 24 aprile 2024 il Dipartimento di Giustizia degli Stati Uniti ha comunicato l'arresto dei due fondatori di Samourai Wallet, che forniva il servizio Whirlpool di CoinJoin, accusati di aver operato senza le necessarie licenze da Money Services Business e di aver favorito il riciclaggio di oltre 100 milioni di dollari provenienti da attività criminali.
Dopo pochi giorni, anche la società ZkSNACKs, che ha sviluppato Wasabi Wallet, ha attivato una serie di azioni:

- dal 1° giugno 2024 ha interrotto il servizio di CoinJoin coordinator che gestiva sul wallet Wasabi Wallet.
- La gestione del codice di Wasabi Wallet, già disponibile in open source, è stata trasferita a un'utenza separata da ZkSNACKs, consentendo a Wasabi Wallet di essere mantenuto come progetto completamente autonomo, indipendente da qualsiasi organizzazione e aperto a molteplici contributori e sostenitori diversi.
- l'impostazione del coordinator è aperta e può essere impostata in modo molto semplice dall'utente, e si è creata una comunità di coordinator e decentralizzando un aspetto critico del suo funzionamento

Coinswap

Livello: avanzato

Argomento: tecnologia

Coinswap è un protocollo che consente a due o più utenti di creare una serie di transazioni che appaiono come pagamenti indipendenti ma che in realtà scambiano le monete tra loro, opzionalmente effettuando un pagamento nel processo. Ciò migliora la privacy non solo degli utenti di coinswap ma di tutti gli utenti di Bitcoin, poiché tutto ciò che sembra un pagamento avrebbe potuto essere invece un coinswap. I coinswaps sono spesso paragonati ai coinjoin, la differenza più ovvia è che un coinjoin utilizza una singola transazione, ma un coinswap utilizza due o più transazioni. Sebbene sia possibile che un coinjoin assomigli a un pagamento batch, può essere abbastanza facile da identificare onchain e alcuni exchange si sono rifiutati di accettare monete con una storia recente di coinjoin. I coinswap sembrano pagamenti, quindi potrebbero essere più difficili da discriminare. I coinswaps possono anche essere eseguiti su diverse blockchain, spesso sotto il nome di atomic swap, cosa non possibile con un coinjoin

Cold channel

Livello: avanzato

Argomento: tecnologia

I Cold channel consentono pagamenti offline con un semplice schema a 2 cicli e un approccio multisig 2 di 2, sebbene siano limitati da denominazioni fisse.

I Cold channel sono il tipo di percorso più semplice che richiede un coordinamento minimo.
Implica uno schema a 2 cicli A-B-A-B e può essere utilizzato in una relazione peer-to-peer tra due entità non professionali.

Cold storage

Livello: base

Argomento: tecnologia

Il cold storage bitcoin è una tecnica di conservazione delle criptovalute che consiste nel mantenere le chiavi private offline, ovvero non connesse a Internet. In questo modo, le chiavi private sono protette da attacchi informatici e da altri rischi di sicurezza.

Tipologie di cold storage Esistono due principali tipologie di cold storage bitcoin:

- Hardware wallet: un dispositivo hardware progettato specificamente per la conservazione delle criptovalute offline. Gli hardware wallet sono dotati di un chip di sicurezza che protegge le chiavi private da accessi non autorizzati.
- Paper wallet: un pezzo di carta o altro materiale su cui viene stampata la chiave privata. I paper wallet sono semplici e convenienti, ma richiedono una maggiore attenzione nel proteggere la chiave privata da furti o danni. Vantaggi del cold storage

Il cold storage offre i seguenti vantaggi:

- Maggiore sicurezza: le chiavi private sono protette da attacchi informatici e da altri rischi di sicurezza.
- Minore probabilità di smarrimento: le chiavi private sono memorizzate offline, quindi sono meno soggette a smarrimento.
- Maggiore controllo: l'utente ha il pieno controllo delle proprie chiavi private. Svantaggi del cold storage

Il cold storage presenta anche alcuni svantaggi:

- Difficoltà di utilizzo: gli hardware wallet possono essere difficili da utilizzare per i principianti.
- Costo: gli hardware wallet possono essere costosi.
- Rischio di perdita: in caso di perdita o danneggiamento del dispositivo di cold storage, si perde l'accesso alle proprie criptovalute se non si è fatta una copia di backup.

Il cold storage è la tecnica di conservazione più sicura per le criptovalute. Tuttavia, è importante essere consapevoli dei suoi svantaggi, in particolare del rischio di perdita delle chiavi private.

In linea di principio, per il cold storage è possibile usare un PC air-gapped ovvero non connesso a Internet, ma non è la soluzione più sicura e più semplice da implementare: un PC per poter fare funzioni di cold storage non dovrebbe essere mai stato connesso a Internet e non dovrebbe essere mai connesso ad internet, altrimenti diventa esposto a potenziali attacchi informatici.

Cold wallet

Livello: base

Argomento: tecnologia

È un wallet che per motivi di sicurezza non è collegato ad Internet.

È un tipo di wallet digitale che opera in modalità offline e, di conseguenza, rientra nella categoria di cold storage. Un cold wallet può assumere varie forme, come un hardware wallet (dispositivo fisico), un paper wallet o addirittura un computer air-gapped ovvero non connesso a Internet dedicato all'archiviazione delle chiavi private.

Collateral

Garanzia

Livello: intermedio

Argomento: finanza

è un modo per garantire il debito e fornire ricorso ai finanziatori quando un debitore o mutuatario è inadempiente su un prestito. Quando un mutuatario vuole ottenere un prestito senza garanzie, un mutuante non può essere sicuro che il mutuatario ripagherà quel prestito. La garanzia aiuta ad aumentare la fiducia tra le controparti per ridurre la possibilità di default. Se il mutuatario è inadempiente, il mutuante può ottenere la proprietà della garanzia fino al rimborso del debito del mutuatario. A volte, il bene stesso diventa una garanzia per un prestito. Ad esempio, un'auto può essere una garanzia per un prestito auto e la casa stessa è una garanzia su un mutuo per la casa. In questi casi, il recupero del bene riduce al minimo il rischio per i finanziatori. I conti di deposito possono anche essere offerti come garanzia.

Collateralization

Livello: avanzato

Argomento: finanza

è l'uso di un bene prezioso (Collateral) per garantire un prestito. Se il mutuatario è inadempiente sul prestito, il mutuante può sequestrare il bene e venderlo per compensare la perdita. La garanzia delle attività offre ai finanziatori un livello sufficiente di rassicurazione contro il rischio di insolvenza. Aiuta anche alcuni mutuatari a ottenere prestiti se hanno storie di credito scadenti. I prestiti garantiti generalmente hanno un tasso di interesse sostanzialmente inferiore rispetto ai prestiti non garantiti.

Colored Coins

Livello: avanzato

Argomento: tecnologia

Sviluppato nel 2013, Colored Coins era una proposta che mirava a utilizzare la blockchain Bitcoin per emettere "bitcoin colorati" che potessero rappresentare vari "colori" (cioè varietà) di asset, tra cui valute, azioni e altro.

Il progetto è stato un primo tentativo di creare ciò che oggi chiamiamo token.

Sebbene le Colored Coin non siano mai decollate completamente da sole, hanno ispirato una nuova tecnologia oggi ampiamente utilizzata.

Una Colored Coin è una criptovaluta che include la promessa di un emittente di beni di fornire un bene o un servizio al proprietario della moneta. L'emittente dell'asset crea Colored Coin codificando alcune delle proprie criptovalute con metadati utilizzando uno speciale wallet che sa come colorare le monete.

I metadati specificano gli obblighi dell'emittente del bene nei confronti dei possessori della moneta. Ad esempio, un musicista può emettere Colored Coin che danno ai possessori il diritto di partecipare a un concerto in una data e in un luogo specifici. Tutti coloro che possiedono una delle Colored Coin possono partecipare.

Dopo aver creato le Colored Coin, l'emittente può trasferirle ad altri soggetti. I trasferimenti vengono elaborati come transazioni sulla rete blockchain della criptovaluta, in modo da offrire lo stesso livello di sicurezza e irreversibilità.

commitment

Livello: base

Argomento: tecnologia

Il termine commitment o il corrispondente verbo commit sono termini molto importanti per spiegare alcuni meccanismi fondamentali della crittografia e conseguentemente nei bitcoin e nelle criptovalute, ma non ci sono dei termini italiani con i quali possano essere decentemente tradotti e infatti spesso si usano direttamente i termini inglesi. Potrebbe essere tradotto con *impegno*, o impegno vincolante, anche in considerazione che quando si parla di commit si usa anche il termine binding, vincolante.

Un commitment scheme è una primitiva crittografica che consente di effettuare il commit, o l'impegno, su un valore scelto (o su un'affermazione scelta) tenendolo nascosto agli altri, con la possibilità di rivelare il valore su cui si è fatto il commit in un secondo momento.

I commitment scheme sono progettati in modo che una parte non possa cambiare il valore o l'affermazione dopo aver fatto il commit: in altre parole, i commitment scheme sono vincolanti. I commitment scheme trovano importanti applicazioni in numerosi protocolli crittografici e le Zero-Knowledge Proof.

commitment transaction

transazione di impegno

Livello: avanzato

Argomento: tecnologia

Una commitment transaction, in italiano traducibile in transazione di impegno, è una transazione Bitcoin firmata da entrambi i partner di un canale Lightning Network, che rappresenta l'ultimo saldo del canale, che viene scambiata tra i partnon e viene immediatamente salvata sulla blockchain on-chain.

Ogni volta che viene effettuato o inoltrato un nuovo pagamento utilizzando il canale Lightning, il saldo del canale si aggiorna e viene firmata una nuova commitment transaction con due output spendibili, uno per ogni partner.

Le commitment transaction garantiscono che non sia necessario fidarsi del proprio partner del canale per recuperare il balance del canale in caso di problemi.

Nel caso di un canale tra Alice e Bob, entrambi i partecipanti mantengono una copia della commitment transaction firmata da entrambi.
La chiusura normale di un canale viene effettuata tramite una closing transaction firmata in accordo da entrambi i partner. Tuttavia, sia Alice che Bob possono unilateralmente chiudere il canale in qualsiasi momento inviando una commitment transaction alla blockchain Bitcoin. La rete non è in grado di distinguere se la commitment transaction trasmessa sia la più recente o una più vecchia, ma l'invio di una versione più vecchia e quindi obsoleta della transazione è considerato un comportamento scorretto e può essere sanzionato dall'altro partner attraverso una penalty transaction o transazione di penalità, che gli permette di rivendicare tutti i fondi del canale per sé.

Spesa ritardata (Timelocked) verso se stessi Le commitment transaction sono asimmetriche nel modo in cui gestiscono i fondi in caso di chiusura forzata di un canale Lightning. Se una delle parti tenta di chiudere il canale trasmettendo una vecchia versione della transazione, il partner onesto ha la possibilità di contestare questa azione. In questo scenario:

- I fondi del partner che ha avviato la chiusura forzata (e che ha tentato di trasmettere una transazione obsoleta) vengono indirizzati verso un contratto di arbitrato. Questo contratto impone un periodo di attesa, permettendo al partner onesto di presentare una prova di illecito.
- I fondi del partner onesto vengono invece inviati immediatamente al suo wallet.

Questa asimmetria concede al partner onesto il tempo necessario per confutare la transazione illecita e rivendicare i propri fondi, fornendo così un meccanismo di sicurezza contro comportamenti fraudolenti.

Le fee della commitment transaction vengono impostate durante la negoziazione

della transazione, e non possono essere modificate senza entrambe le firme; poiché non si possono conoscere quali saranno le fee in futuro per consentire di confermare la transazione in tempo, possono essere impostate con un importo significativamente più alto, fino a cinque volte, rispetto alle stime al momento della negoziazione.

La commitment transaction include output aggiuntivi per eventuali HTLC in sospeso, rendendola più grande in termini di byte rispetto a una closing transaction di chiusura reciproca.
Di solito questo non sarebbe troppo grave.
Ma se c'è un congestionamento della rete, con molti HTLC in attesa che devono essere inclusi nella transazione, la transazione può avere delle dimensioni tali che con un mercato di fee molto alto potrebbero portare ad avere delle fee superiori all'intero balance del canale.

I due output sono chiamati:

- to_local
- to_remote

Questo il codice script del primo output (to_local) di una commitment transaction:

```
OP_IF
    # Penalty transaction
    <revocationpubkey>
OP_ELSE
    `to_self_delay`
    OP_CHECKSEQUENCEVERIFY
    OP_DROP
    <local_delayedpubkey>
OP_ENDIF
OP_CHECKSIG
```

Questo script ha 2 condizioni, e l'importo può essere speso se viene soddisfatta una delle due possibili condizioni:

- firmare la *revocationpubkey*
- firmare la *local_delayedpubkey* dopo un numero di blocchi specificati in *to_self_delay*

Commodity

Livello: intermedio

Argomento: economia

Nel settore Bitcoin e cripto, il termini Commodity e Security vengono utilizzati spesso in contrapposizione per definire una criptovaluta. In questo contesto, generalmente viene utilizzato il seguente significato:

- **Commodity**: bene tangibile, il cui valore sottostante è dato dall'utilità percepita come mezzo di pagamento, riserva di valore o strumento di investimento.
- **Security**: titolo che rappresenta una partecipazione o un credito nei confronti di una organizzazione o una società, il cui valore sottostante è dato dall'utilità percepita di quell'organizzazione o società.

Si sta affermando la posizione secondo la quale Bitcoin sia una commodity, e tutte le altre cripto security.

Commodity è un termine inglese che indica un bene per cui c'è domanda ma che è offerto senza differenze qualitative sul mercato ed è fungibile, cioè il prodotto è lo stesso indipendentemente da chi lo produce, come per esempio il petrolio o i metalli.

Nel settore delle cripto si cerca di identificare se coin o token vanno considerati come security o come commodity, perché gli adempimenti richiesti per l'emissione e la vendita di token di tipo security sono molto più impegnativi rispetto a quelli di tipo commodity.
I token di tipo commodity in certi casi possono essere definiti come utility token.

Anche le agenzie governative americane si sono espresse considerando Bitcoin come commodity e la maggior parte delle altre cripto security.

L'agenzia statunitense di riferimento per le commodity è la CFTC. A giugno 2022 Gary Gensler, il presidente della SEC, l'ente federale statunitense preposto alla vigilanza della borsa valori e delle security, parlando di criptovalute ha definito Bitcoin come commodity: *"Alcune, come Bitcoin, e questo è l'unica che posso dire… sono commodities"*

ipotizzando che la maggior parte delle coin e token siano security:

"Dei circa 10.000 token presenti sul mercato delle criptovalute la stragrande maggioranza è costituita da security. Le offerte e le vendite di queste migliaia di security token sono coperte dalle leggi sulle security. Alcuni token potrebbero non soddisfare la definizione di security - quelli che chiamerò crypto non-security token. Questi rappresentano probabilmente solo un piccolo numero di token, anche se possono rappresentare una parte significativa del valore aggregato del mercato delle criptovalute."

Crypto-commodity è un termine generico usato per descrivere un asset negoziabile o fungibile che può rappresentare un bene, un'utilità o un contratto nel mondo reale o virtuale attraverso token esclusivi su una rete blockchain.

Common Input Ownership Heuristic

Euristica della proprietà comune degli input

Livello: avanzato

Argomento: legale

La Common Input Ownership Heuristic, euristica della proprietà comune degli input in italiano, è un metodo utilizzato per analizzare le transazioni in Bitcoin e dedurre relazioni tra gli indirizzi.

La sua base è l'ipotesi che se due transazioni condividono un input in comune, è possibile che quell'input appartenga allo stesso proprietario. Questo perché in Bitcoin, un indirizzo può spendere solo le sue entrate, quindi se due transazioni condividono un input, è probabile che appartengano allo stesso indirizzo.

È una delle principali euristiche utilizzate dalle società di Chain Analysis per determinare il proprietario di specifici UTXO. Questa euristica attualmente presuppone che tutti gli input di una determinata transazione siano di proprietà dello stesso proprietario.

L'euristica viene utilizzata in diverse analisi di tracciabilità e ricerca su Bitcoin, ma non è una tecnica infallibile poiché può essere ingannata tramite tecniche come Coinjoin o Payjoin. In questi casi, più indirizzi appartenenti a proprietari diversi condividono lo stesso input, rendendo più difficile l'analisi delle transazioni.

Questa euristica non ha mai offerto certezze e, con la continua evoluzione del Bitcoin, sta diventando sempre meno affidabile. Oltre a CoinJoin, CoinSwap, Multisig regolare e, in futuro, le transazioni MuSig contraddicono questa euristica accettando input da molte parti diverse.

Confirmation

Conferma

Livello: base

Argomento: tecnologia

Si indica come "confermata" una transazione che è stata inserita in un blocco della blockchain.

Ogni nuovo blocco che viene aggiunto al blocco contenente la transazione, incrementa il numero di conferme.

Così ad esempio se dopo il blocco contenente la transazione sono stati aggiunti ulteriori 5 blocchi nella blockchain, la transazione ha 6 conferme.

È importante attendere la conferma di una transazione per evitare double spending o attacchi tipo il Race Attack.

Maggiore è il numero di conferme, e più diventa difficile se non addirittura impossibile modificare il blocco e quindi la transazione, perché una modifica di un blocco richiederebbe la riscrittura di tutti i blocchi successivi e il relativo lavoro fatto dai miner.

Nel caso della blockchain bitcoin, dove viene minato in media un blocco ogni 10 minuti, per avere 6 conferme è necessario che passi in media un ora.

Consensus cleanup soft fork

Livello: avanzato

Argomento: tecnologia

Il Consensus cleanup soft fork, o soft fork di pulizia del consenso, è una proposta per affrontare diversi problemi nelle regole di consenso di Bitcoin che risalgono alla versione originale di Bitcoin rilasciata nel 2009.

Le discussioni sulla tecnologia blockchain, in particolare nell'ambito del framework di Bitcoin, mette in evidenza diversi settori chiave di attenzione mirati a potenziare la sicurezza e la funzionalità della rete.

Una proposta di emendamento per garantire l'unicità dell'ID della transazione (txid) prevede di richiedere che i blocchi con più di una transazione includano un witness commitment da un'altezza di blocco futura specificata, esentando i blocchi vuoti. Questa misura è progettata per prevenire problemi come le transazioni duplicate di coinbase, identificate in contesti storici a specifiche altezze di blocco, consentendo contemporaneamente al software di mining di adattarsi nel tempo.

Ulteriori discussioni approfondiscono l'ottimizzazione dei processi di convalida della blockchain e l'utilizzo di meccanismi come SIGHASH_SINGLE. Il riconoscimento delle soluzioni esistenti come Taproot insieme a miglioramenti potenziali, come modifiche alla dimensione del campo nonce, riflette un impegno continuo nel bilanciare l'efficienza operativa con la sicurezza della rete. Inoltre, gli aspetti teorici delle biforcazioni soft e i loro limiti nell'applicare retrospettivamente regole mettono in evidenza le complessità nel mantenere la robustezza e l'adattabilità della blockchain.

Le considerazioni tecniche si estendono al mantenimento dell'integrità della blockchain attraverso meccanismi unici per i blocchi vuoti, enfatizzando il ruolo del "valore riservato al witness" e del witness commitment. Inoltre, l'esplorazione del tracciamento delle altezze dei blocchi sottolinea le sfide nel garantire scalabilità e sicurezza a lungo termine, con un collegamento fornito per illustrare possibili violazioni future.

Le strategie per mitigare i processi lenti di convalida all'interno della rete Bitcoin propongono la convalida parallela dei punteggi concorrenti della blockchain, anche se vengono evidenziate preoccupazioni sulla coordinazione e il suo impatto sulla decentralizzazione. La discussione affronta anche il caso estremo dei tempi di convalida dei blocchi e le strategie per mantenere l'integrità della rete senza compromettere gli asset, richiedendo il feedback della comunità per perfezionare questi approcci.

Infine, viene esaminata la proposta di Matt Corallo per la Grande Pulizia del Consenso, identificando vulnerabilità nel protocollo Bitcoin e suggerendo miglio-

ramenti che vanno dall'affrontare la vulnerabilità del timewarp al potenziamento dell'efficienza delle transazioni non-SegWit. La proposta cerca il contributo della comunità per affrontare bug e inefficienze, con l'obiettivo di rafforzare il design e il funzionamento di Bitcoin in modo collaborativo.

Consensus Mechanism

Meccanismo di Consenso

Livello: intermedio

Argomento: tecnologia

È un sistema per ottenere un consenso tra i partecipanti ad una rete sullo stato o sui dati. Nel caso delle blockchain, si riferisce spesso al meccanismo che consente ai partecipanti di aggiungere un blocco perché considerato valido. Nel caso di Bitcoin, si parla di Nakamoto Consensus per il quale viene utilizzato la PoW.

I metodi di consenso blockchain mitigano la sfida nel raggiungere il consenso in un mondo digitale distribuito a livello globale, consentendo agli utenti di convalidare le voci nel ledger della blockchain, aiutando a sincronizzare i dati e rafforzando la sicurezza della rete. Tali metodi devono garantire che tutti i partecipanti alla rete possano concordare su un'unica fonte di "verità", anche se alcuni nodi si guastano; in altre parole, devono essere Byzantine Fault Tolerant (BFT). Il concetto di BFT deriva dal Problema dei Generali Bizantini, un problema di teoria dei giochi che descrive la difficoltà dei partecipanti ad un sistema decentralizzato nel raggiungere il consenso senza affidarsi a una parte centrale fidata. Inizialmente concepito nel 1982 come un dilemma logico, un gruppo di generali bizantini deve coordinare perfettamente un attacco, con l'aggravante di non poter comunicare direttamente tra loro.

consolidation

consolidamento

Livello: intermedio

Argomento: tecnologia

Con consolidamento del wallet, consolidation in inglese, si intende un'operazione che consiste nel raggruppare più output o UTXO in una unico UTXO, inviando tutti i Bitcoin presenti in un portafoglio ad un unico indirizzo Bitcoin. Questo processo comporta la riduzione del numero di input nel portafoglio, rendendolo più efficiente e sicuro.

Vantaggi del consolidamento del portafoglio:

- Minori fee di transazione: due transazioni anche se spendono un importo uguale, possono pesare di più e conseguentemente costare di più in termini di fee, in base agli input e agli output coinvolti. Se l'importo disponibile nel

proprio portafogio è molto frammentato, sarà necessario mettere insieme diversi input per raggiungere un certo importo.
- Maggiore privacy: Riduce il numero di informazioni tracciabili sulla blockchain, rendendo più difficile risalire ai tuoi movimenti di Bitcoin.
- Maggiore organizzazione: Può rendere il tuo portafoglio Bitcoin più organizzato e facile da gestire.

Esistono diversi modi per consolidare il proprio wallet Bitcoin.

È ad esempio sufficiente inviare tutto l'ammontare presente nel proprio wallet ad un proprio indirizzo Bitcoin. In questo modo si andranno a ridurre il numero di input presenti nel wallet e di conseguenza anche il peso in kilobyte.
Questa operazione è da effettuarsi preferibilmente quando le fee sono basse; può infatti verificarsi il paradosso che alcuni UTXO possano avere importi inferiori alle fee necessarie per trasferirli, rendendo antieconomico l'operazione di consolidamento per questi UTXO; questi output di scarso valore possono essere definiti come Uneconomical outputs o Dust.

Cooldown

Livello: avanzato

Argomento: tecnologia

Il Cooldown nel processo di mining è il termine utilizzato per indicare il periodo di tempo nel quale non è consentito spendere (o più precisamente trasferire) i nuovi bitcoin coniati dai miner nella transazione coinbase di ogni blocco.

Questo periodo di tempo corrisponde a 100 blocchi. Considerato che mediamente viene minato un blocco ogni 10 minuti, questo tempo è circa di 1000 minuti.

Counterparty

Livello: avanzato

Argomento: tecnologia

Counterparty è una piattaforma peer-to-peer e un protocollo Internet distribuito e open source costruito sulla base della blockchain e della rete Bitcoin.

È stata una delle più note piattaforme Bitcoin di secondo livello per la creazione di asset e NFT nel 2014.

Si tratta di un protocollo di tipo *metacoin*.

Offre caratteristiche quali valute negoziabili create dall'utente, strumenti finanziari aggiuntivi e uno scambio decentralizzato di asset.

Nel novembre 2014, Counterparty ha aggiunto al protocollo Counterparty il supporto per la Ethereum Virtual Machine, consentendo a tutte le applicazioni

decentralizzate Ethereum di essere eseguite sulla blockchain Bitcoin all'interno del protocollo Counterparty.

covenant

Livello: avanzato

Argomento: tecnologia

Attualmente, una transazione Bitcoin funziona nel seguente modo: quando si possiedono dei bitcoin bloccati in un determinato output e si vuole sbloccarli per utilizzarli, si crea una nuova transazione che dimostra che si ha la capacità di farlo.
Questa dimostrazione può avvenire attraverso la presentazione di una firma digitale valida, un hash corrispondente, o altri metodi.

Tuttavia, una volta dimostrato di avere il diritto di sbloccare quei bitcoin, si diventa il proprietario di tali bitcoin sbloccati e si è liberi di utilizzarli come si desidera. Non ci sono ulteriori restrizioni sull'uso di tali bitcoin.

Il concetto di "covenant" si riferisce a un tipo specifico di restrizione che può essere applicata a una transazione Bitcoin. Invece di limitarsi a seguire le istruzioni necessarie per sbloccare i bitcoin, il covenant richiede che anche la transazione risultante dallo sblocco dei bitcoin rispetti determinate limitazioni.

Un esempio tipico di covenant è il Check Template Verify (CTV).
Con il CTV, ad esempio, si può creare una condizione di sblocco che richiede che quando si sbloccano degli output, si possa creare solo una nuova transazione il cui hash sia compreso in una lista predefinita di hash, che rappresenta i template.

I Covenant sono una categoria di modifiche proposte alle regole di consenso di Bitcoin che consentirebbero a uno script di impedire a uno spender autorizzato di spendere a determinati altri script.

Nel contesto di Bitcoin, la definizione più utile di covenant è quando la scriptPubKey di un UTXO limita la scriptPubKey nel o negli output di una transazione che spende quell'UTXO.

Ad esempio, un Covenant può normalmente consentire la spesa solo a un insieme di script inseriti in una whitelist, come la restituzione di bitcoin al saldo dello stesso utente o la spesa a un indirizzo che consente la spesa a qualsiasi indirizzo arbitrario solo dopo un certo periodo di tempo.

CPFP

Acronimo di: Child pays for parent

Livello: avanzato

Argomento: tecnologia

CPFP, o *Child pays for parent* che tradotto letteralmente in italiano sarebbe *Il figlio paga per il genitore*, è una tecnica per incoraggiare i miner a confermare, ovvero inserire in blockchain, una transazione che avendo delle fee poco competitive con le altre transazioni tarda ad essere inserita in blockchain.

Diversamente da RBF, una tecnica analoga, dove chi ha creato la transazione che non è stata ancora inserita in blockchain può riproporla con fee più alte, con CPFP può essere il destinatario del pagamento che può creare una nuova transazione per spendere parte dell'importo che deve ricevere.

L'utente quindi spende un output UTXO da una transazione non confermata con basse fee in una transazione figlio con una fee elevata per incoraggiare i miner a includere entrambe le transazioni in un blocco.

Le regole di consenso di Bitcoin richiedono che la transazione che crea un output appaia prima nella catena di blocchi rispetto alla transazione che spende tali output, incluso che la transazione genitore appaia prima nello stesso blocco rispetto alla transazione figlio se entrambe sono incluse nello stesso blocco.

Ciò significa che una transazione non confermata con una commissione elevata può incentivare i miner a minare qualsiasi transazione precedente non confermata.

La differenza con RBF può quindi essere così riassunta:

- RBF consente al mittente di incrementare le fee per ottenere la conferma della transazione più velocemente. Utilizzate RBF se siete il mittente che ha bisogno di velocizzare la transazione.
- CPFP consente al destinatario creando una nuova transazione di pagare per ottenere la conferma della transazione più velocemente. Usate il CPFP se siete il destinatario che ha bisogno di velocizzare la transazione.

CPFP carve out

Livello: avanzato

Argomento: tecnologia

Il **CPFP carve out** è una politica di transaction relay implementata in Bitcoin Core che consente a una singola transazione di superare moderatamente i limiti massimi di dimensione e profondità del pacchetto del nodo se tale transazione ha un solo antenato non confermato.

Ciò consente ai protocolli di contratto a due parti (come l'attuale protocollo Lightning Network) di garantire a entrambe le parti la possibilità di utilizzare il fee bumping del Child Pays For Parent CPFP. La prima parte può usare il fee bumping fino ai limiti del pacchetto, ma non può bloccare la transazione perché la seconda parte può usare il **CPFP carve out**.

CPI

Acronimo di: Consumer Price Index

Indice dei prezzi al consumo

Livello: intermedio

Argomento: economia

L'indice dei prezzi al consumo è un indicatore dei prezzi di un paniere di beni e servizi di base, è una misura del costo della vita e viene utilizzato per valutare l'inflazione

Il paniere include beni e servizi di consumo tra cui trasporto, cibo, cure mediche e costi associati alla vita in una zona specifica. È determinato dall'aggregazione dei prezzi medi di un paniere di articoli, ed è generalmente usato per identificare i periodi di inflazione o deflazione e l'efficienza complessiva delle politiche economiche di un governo. Tipicamente coinvolge statistiche che coprono coloro che sono impiegati, lavoratori autonomi, disoccupati, pensionati, incarcerati, impoveriti, e altro. Il CPI non riflette perfettamente i cambiamenti dei prezzi. Il CPI non tiene conto delle sostituzioni che i consumatori fanno in base ai prezzi. Se un bene diventa significativamente più costoso, i consumatori semplicemente ne compreranno meno, sostituendolo con un bene simile che è più economico; per tenere conto dell'innovazione tecnologica e dei beni di nuova creazione richiede degli interventi di modifica della sua composizione, per mantenere il suo paniere coerente nel tempo.

CPU

Acronimo di: Central Processing Unit

Unità di elaborazione centrale

Livello: base

Argomento: tecnologia

nota anche come processore, è definita come il "cervello" centrale del computer, che coordina diversi componenti in esecuzione. Si distingue da altri tipi di processori per il fatto di essere adatta ai diversi tipi di elaborazione, rispetto ad esempio a chip dedicati come la GPU che è specializzata nell'eseguire più velocemente, rispetto alla CPU, calcoli necessari per la grafica e per elaborare immagini, o dagli Asic che sono ancora più specializzati per un solo tipo di calcolo. Questa specializzazione viene sfruttata per elaborare anche alcuni calcoli effettuati dai miner , rendendo in alcuni casi l'uso della CPU non competitivo per il raggiungimento dello scopo.

Cripto-attività

Livello: intermedio

Argomento: economia

Il termine Cripto-attività potrebbe essere usato in modo intercambiabile con il termine inglese Crypto-asset, ma possono esistere delle differenze tra il significato di questi due termini analogamente a quanto accade tra i termini Attività e Asset.

Il termine Cripto-attività ha anche fatto il suo ingresso nel Testo Unico delle Imposte Dirette, con la legge 29 dicembre 2022 n. 197 che contiene alcune disposizioni riguardanti la tassazione delle Cripto-attività, nella quale viene così definita:

Ai fini della presente lettera, per "cripto-attività" si intende una rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga. Non costituisce una fattispecie fiscalmente rilevante la permuta tra cripto-attività aventi eguali caratteristiche e funzioni.

Definizione mutuata dalla provvisoria definizione prevista dalla proposta de regolamento europeo MiCA.

Il concetto di Cripto-attività comprende sia valute virtuali quali Bitcoin, Ethereum e Stablecoin (quali USD Tether e USD Coin), sia tutte le altre rappresentazioni digitali di valore o diritti che utilizzano la tecnologia di registro distribuito, formando una definizione ampia a fini fiscali.

Crittografia

Livello: base

Argomento: tecnologia

Si tratta di quella branca della matematica che ci consente di creare prove matematiche che consentono di proteggere le informazioni dalle eventuali azioni di attackers. La crittografia, nata in ambito militare, è ampiamente usata nel commercio, nelle operazioni bancarie online o nelle app di messaggistica ed è alla base di diverse funzioni necessarie per il funzionamento delle criptovalute.

Bitcoin utilizza la matematica crittografica in tutto il suo progetto per consentire ai partecipanti di controllare il comportamento di tutti gli altri senza fidarsi di una parte centrale.

Crypto

Livello: base

Argomento: tecnologia

il termine viene usato a volte come abbreviazione di Cryptocurrency , o come indicatore di tutto il settore delle criptovalute.

Crypto asset

Livello: intermedio

Argomento: politica

Secondo la proposta del MiCA i crypto-asset sono definiti come una rappresentazione digitale di valore o diritti che può essere trasferita e memorizzata elettronicamente, utilizzando la DLT, tecnologia dei distributed ledger o una tecnologia simile:

I cripto-asset sono una delle principali applicazioni delle DLT. I cripto-asset sono rappresentazioni digitali di valore o di diritti che hanno il potenziale per portare benefici significativi sia agli operatori di mercato partecipanti al mercato e ai detentori al dettaglio di cripto-asset. La rappresentazione del valore include anche il valore esterno, valore esterno e non intrinseco attribuito a un cripto-asset dalle parti interessate o dai partecipanti al mercato, il che significa che il valore può essere soggettivo e può essere attribuito soltanto all'interesse di chi acquistare il cripto-asset. Semplificando i processi di raccolta di capitali e aumentando la concorrenza, le offerte di cripto-asset possono consentire un modo innovativo e inclusivo di finanziamento, anche per le piccole e medie imprese. Se utilizzati come mezzo di pagamento, i token di pagamento possono presentare opportunità in termini di pagamenti più economici, più rapidi e più efficienti, in particolare a livello transfrontaliero, limitando il numero di intermediari.

Si prevede che molte applicazioni della DLT, tra cui la tecnologia blockchain, che non sono ancora state studiate a fondo, creeranno nuovi tipi di attività e modelli di business che, insieme allo stesso settore dei cripto-asset, porteranno alla crescita economica e a nuove opportunità di lavoro per i cittadini dell'Unione.

I cripto-asset rientrano nell'ambito di applicazione della vigente normativa dell'UE in materia di servizi finanziari, in particolare quelli che si qualificano come strumenti finanziari ai sensi della direttiva 2014/65/UE del Parlamento europeo e del Consiglio. Agli emittenti di tali cripto-asset si applica una serie completa di norme dell'Unione agli emittenti di tali cripto-asset e alle imprese che svolgono attività connesse a tali cripto-asset.

Altri cripto-asset, tuttavia, non rientrano nell'ambito di applicazione della legislazione dell'Unione sui servizi finanziari. Non esistono norme, oltre a quelle antiriciclaggio, per i servizi relativi a questi cripto-asset non regolamentati, compresa la gestione di piattaforme di negoziazione di cripto-asset, il servizio di scambio di cripto-asset con fondi o altri cripto-asset o la custodia di cripto-asset.

I cripto asset vengono divisi da MiCA in queste categorie:

- **EMTs e-money tokens**
- **ARTs Asset-referenced token**

- **Utility Token**

Crypto winter

Livello: intermedio

Argomento: finanza

Con Crypto winter, o inverno delle cripto, si intende un periodo di settimane o mesi nel quale i prezzi delle cripto sono scesi molto e poi sono rimasti bassi.

La frase "crypto winter" probabilmente proviene dalla serie della HBO, "Game of Thrones" nella quale il motto della House of Stark era "Winter Is Coming", l'inverno sta arrivando. Era considerato un avvertimento che un conflitto duraturo poteva calare sulla terra di Westeros in qualsiasi momento.

Allo stesso modo, possono arrivare e arrivano dei lunghi periodi nei quali i prezzi delle criptovalute rimangono molto bassi rispetto ai massimi storici, o ATH, o in caduta.

Definindo la frase in modo letterale, il crypto winter avviene quando i prezzi si contraggono e rimangono bassi per un lungo periodo.

Ad esempio il periodo da gennaio 2018 a dicembre 2020 viene considerato un Crypto winter, durato quasi tre anni.

Durante questi periodi, generalmente molte aziende collegate ad attività cripto entrano in crisi e tra queste molte chiudono.

Cryptocurrency

Criptovaluta

Livello: base

Argomento: tecnologia

Con cryptocurrency, in italiano criptovaluta, si intende un tipo di valuta digitale protetta dalla crittografia e, in genere, utilizzata come mezzo di scambio all'interno di un sistema economico digitale peer-to-peer (P2P).

L'uso di tecniche crittografiche è ciò che garantisce che questi sistemi siano completamente immuni da frodi e contraffazioni.

La prima criptovaluta ad essere mai creata è stata Bitcoin, introdotta dallo sviluppatore pseudonimo Satoshi Nakamoto, nel 2009. L'obiettivo di Nakamoto era creare un nuovo sistema di pagamento elettronico che consenta transazioni finanziarie digitali tra utenti senza la necessità di intermediari, come banche o istituzioni governative.

La creazione del termine cryptocurrency è stato attribuito allo stesso Satoshi Nakamoto, ma in un'e-mail che Nakamoto ha inviato a Martti Malmi sembra

aprire un buco importante in questa teoria.

Secondo Satoshi: “Qualcuno ha inventato la parola ‘cryptocurrency’. … Forse è una parola che dovremmo usare per descrivere Bitcoin, ti piace?”.

La maggior parte dei sistemi di criptovaluta funziona attraverso un framework decentralizzato gestito collettivamente da una rete distribuita di computer.

CryptoKitties

Cripto gattini

Livello: intermedio

Argomento: tecnologia

sono considerati uno dei primissimi casi di successo nell’uso degli NFT . È un gioco virtuale, una sorta di Tamagotchi online che consente ai giocatori di comprare gattini in forma di NFT su blockchain Ethereum, e attraverso la possibilità di accoppiamento tra questi NFT generarne dei nuovi con caratteristiche ereditate dagli NFT genitori, e rivenderli ad altri utenti.

CSFS

Acronimo di: OP_CHECKSIGFROMSTACKVERIFY

Livello: avanzato

Argomento: tecnologia

OP_CHECKSIGFROMSTACKVERIFY, OP_CHECKSIGFROMSTACK, OP_CSFS o più semplicemente CSFS, è un un opcode che consente di verificare un messaggio arbitrario rispetto a una firma. Può essere utilizzato per implementare una varietà di nuove funzionalità in Bitcoin, come ad esempio:

- Pagamento delle firme
- Delega
- Oracoli
- Vincoli di protezione da doppia spesa
- Introspezione delle transazioni

OP_CSFS ha il vantaggio di essere generico e flessibile, ma può anche aumentare la dimensione delle transazioni. Spesso viene proposto insieme a OP_CAT, che consente di concatenare due elementi insieme.

È un opcode su sidechain basate su ElementsProject.org che viene talvolta proposto per l’implementazione su Bitcoin. Questo opcode consente di verificare se una firma abbia firmato un messaggio arbitrario. L’opcode richiede tre parametri: una firma, un messaggio e una chiave pubblica.

Gli opcode esistenti di verifica delle firme di Bitcoin, come OP_CHECKSIG, non consentono di specificare un messaggio arbitrario. Il messaggio che utiliz-

zano è derivato dalla transazione che esegue l'opcode di verifica della firma. Ciò consente di verificare che la firma corrisponda a una determinata chiave pubblica e che la chiave privata utilizzata per generare entrambi gli oggetti sia stata utilizzata per autorizzare la spesa. Questo meccanismo è abbastanza potente per garantire la sicurezza degli UTXO di Bitcoin, ma impedisce di utilizzare firme digitali per autenticare altri tipi di dati nel sistema Bitcoin. La capacità di utilizzare OP_CSFS per verificare un messaggio arbitrario può consentire diverse nuove funzionalità per gli utenti di Bitcoin:

- **Pagamento delle firme**: se Alice controlla una chiave privata che può firmare una transazione di pagamento a Bob, Bob può utilizzare OP_CSFS per offrire in modo affidabile di pagare Alice per la firma di cui ha bisogno. Recentemente, i protocolli che coinvolgono il pagamento delle firme assumono tipicamente l'uso di firme adattabili che sono più private e utilizzano meno spazio di blocco.

- **Delega**: Alice potrebbe voler delegare l'autorità di spendere le sue monete a Bob senza creare esplicitamente una transazione onchain che trasferisce le monete a un multisig 1-su-2 tra lei e Bob. Se Alice progetta i suoi script con questo tipo di delega in mente, può inserire la chiave pubblica di Bob in un messaggio e utilizzare OP_CSFS per dimostrare che ha delegato l'autorità di spesa a quella chiave.
  Un approccio alternativo più privato, più flessibile ed efficiente in termini di spazio di blocco è graftroot, anche se ciò richiede un soft fork che finora è stato solo appena discusso.

- Oracoli: un oracolo può accettare di firmare un messaggio che indica l'esito di un evento, ad esempio il nome della squadra nazionale che vince un evento sportivo. Due o più utenti possono quindi depositare denaro in uno script utilizzando OP_CSFS che pagherà una persona diversa a seconda della squadra che l'oracolo indica come vincitrice.
  L'attenzione più recente sui contratti moderati dagli oracoli coinvolge l'uso di contratti a log discreto (DLC), che possono essere più privati ed efficienti in termini di spazio di blocco.

- **Bond di protezione contro la doppia spesa**: un servizio può promettere di non cercare mai di spendere due volte i suoi UTXO al fine di incoraggiare i beneficiari ad accettare le sue transazioni non confermate come pagamenti affidabili. Per dimostrare la sua buona fede, il servizio può utilizzare OP_CSFS per offrire il pagamento di un bond a qualsiasi utente che riesca a dimostrare che la stessa chiave è stata utilizzata per creare due firme diverse per transazioni che spendono lo stesso UTXO. Questo utilizzo di OP_CSFS può essere paragonato a firme a singolo utilizzo che consentono a chiunque veda due firme dalla stessa chiave di derivare la chiave privata utilizzata per crearle, consentendo loro di spendere altri fondi protetti da quella chiave.

- **Introspezione della transazione**: se la stessa coppia di chiave pubblica

e firma è valida sia con OP_CSFS che con OP_CHECKSIG, allora il contenuto del messaggio arbitrario passato a OP_CSFS è identico alla transazione di spesa serializzata (e altri dati) implicitamente utilizzata con OP_CHECKSIG. Questo rende possibile inserire una copia convalidata della transazione di spesa nello stack di valutazione dello script, dove altri opcode possono eseguire test su di essa al fine di imporre restrizioni sulla transazione di spesa.
Ad esempio, se OP_CSFS fosse stato disponibile nel 2015 e nel 2016, sarebbe stato possibile implementare le funzionalità di BIP65 OP_CHECKLOCKTIMEVERIFY CLTV e BIP112 OP_CHECKSEQUENCEVERIFY CSV senza alcuna modifica del consenso semplicemente scrivendo uno script di verifica.
Guardando avanti, OP_CSFS potrebbe anche consentire agli script di implementare le funzionalità dell'hash di firma proposto SIGHASH_ANYPREVOUT, così come altre proposte di opcode come OP_CHECKTEMPLATEVERIFY.
Inoltre, OP_CSFS consentirebbe la creazione di vincoli che limitano il modo in cui un insieme di bitcoin può essere speso, ad esempio, una cassaforte potrebbe limitare la transazione di spesa a un piccolo insieme di scriptPubKeys accettabili per limitare il rischio di furto.
Il punto di forza di OP_CSFS è che fornisce una piena introspezione della transazione di firma in modo completamente generico. Il suo punto debole è che richiede essenzialmente l'aggiunta di una copia completa della transazione di firma allo stack, il che potrebbe aumentare significativamente le dimensioni delle transazioni che desiderano utilizzare OP_CSFS per l'introspezione. In confronto, gli opcode di introspezione a scopo specifico come CLTV e CSV richiedono un overhead minimo, ma l'aggiunta di ciascun nuovo opcode di introspezione speciale richiede una modifica del consenso e potrebbe non essere possibile disabilitarne l'uso (anche se diventano impopolari) senza correre il rischio che qualcuno perda denaro.

CSV (protocols)

Acronimo di: Client-Side Validation

validazione lato cliente

Livello: avanzato

Argomento: tecnologia

Il termine CSV come sigla di client-side validation, in italiano Validazione Lato Client, (da non confondere con CSV Check Sequence Verify del BIP 112) si riferisce ad una modalità di gestione della verifica delle side-chain.

La maggior parte delle blockchain pubbliche esistenti operano con un modello di consenso globale, in cui tutti i nodi validano tutte le transazioni, condividono le informazioni sulle transazioni tra loro e mantengono uno stato globale unificato.

Tuttavia, questo modello presenta una serie di sfide, tra cui:

- Limitazioni di scalabilità che rendono costoso convalidare tutte le interazioni contrattuali;
- Costi elevati che portano a un'operazione centralizzata dei nodi;
- Mancanza di privacy a causa delle informazioni di transazione aperte.

La Validazione Lato Client (CSV) propone un approccio alternativo: richiede solo al livello di consenso di adempiere agli impegni crittografici associati agli eventi del ledger, mentre memorizza le informazioni effettive sugli eventi (il ledger) fuori dalla blockchain.

Questo approccio, che origina dal lavoro di Peter Todd, è definito "Validazione Lato Client". CSV sposta i dati di transazione fuori dalla blockchain, dove vengono archiviati e verificati i dettagli, e solo le informazioni minime vengono inviate sulla blockchain. Inoltre, i dati di transazione vengono trasferiti fuori dalla blockchain solo tra il mittente e il destinatario. Ad esempio, in una transazione del mondo reale, la convalida è richiesta solo quando il wallet e le parti richiedono l'accesso ai dati del contratto.

Caratteristiche chiave di CSV:

- Le informazioni dettagliate sulle transazioni vengono archiviate fuori dalla blockchain e validate solo sul client;
- Solo gli impegni ai dati di transazione vengono archiviati sulla catena;
- La convalida si applica solo alle transazioni di cui gli utenti devono essere a conoscenza.

La CSV può sfruttare le regole di consenso, come ad esempio permettere che un output venga speso una sola volta all'interno di una block chain valida, ma può anche imporre regole aggiuntive conosciute solo da coloro interessati alla convalida.

Un protocollo di CSV concettualmente semplice potrebbe associare un token a un particolare UTXO. Solo l'insieme dei validatori deve essere a conoscenza di tale associazione; non è necessario pubblicarla sulla block chain o in qualsiasi altro luogo pubblico. Quando l'UTXO viene speso, la transazione di spesa associa il token a un nuovo UTXO.
Se Alice attualmente controlla l'UTXO associato al token e Bob desidera acquistarlo da lei, può fornirgli una prova dell'associazione originale, e poi lui può utilizzare la sua copia convalidata della block chain più la CSV per verificare la storia di ogni trasferimento del token fino ad Alice. Può anche verificare che una transazione creata da Alice sia correttamente formattata per assegnare il token a un UTXO che Bob controlla.

Esempi di protocolli CSV sono:

- RGB
- Taproot Assets, precedentemente chiamato Taro

Entrambi i protocolli sono progettati per essere compatibili con transazioni off-chain, come i pagamenti tramite Lightning Network. Similmente al ciclo di vita di un canale Lightning, viene pubblicata una transazione di setup on-chain che vincola i token al controllo condiviso delle parti coinvolte; una serie di transazioni off-chain ciascuna vincola l'allocazione attuale dei token tra le parti; e una transazione contenente l'impegno finale viene pubblicata on-chain.

Solo i wallet che desiderano supportare gli RGB o gli Asset Taproot devono comprendere il protocollo, e solo un wallet che vuole inviare o ricevere un token specifico o un altro contratto di convalida lato client deve sapere qualcosa su tale contratto. Per tutti gli altri, le transazioni create con RGB e Asset Taproot sembrano transazioni Bitcoin regolari.

CTLC

Acronimo di: Covenant Time Locked Contract

Livello: avanzato

Argomento: tecnologia

I CTLC, Covenant Time Locked Contract o Contratti Covenant a tempo limitato, in particolare la variante Optimistic PathCoin, consentono canali di pagamento spontanei senza pre-coordinamento, ma a scapito della privacy e dell'utilizzo invariato dello spazio sulla catena.

Currency

Valuta

Livello: base

Argomento: politica

Currency può essere tradotto in italiano con Valuta. Può essere anche usato il termine Moneta, che in italiano si riferisce però anche all'oggetto fisico.

La valuta è un mezzo di scambio per beni e servizi. In breve, è denaro, sotto forma di carta e monete, solitamente emesso da un governo e generalmente accettato al suo valore nominale come metodo di pagamento.

È il principale mezzo di scambio nel mondo moderno, avendo da tempo sostituito il baratto come mezzo di scambio di beni e servizi.

Nel 21° secolo, una nuova forma di valuta è entrata nel vocabolario e nel regno degli scambi: cryptocurrency, le criptovalute a volte definite anche come valuta virtuale, e a volte Crypto asset ad esempio dal MiCA il regolamento Europeo sui mercati nelle criptovalute.

Le criptovalute, come Bitcoin ed Ethereum, non hanno una forma fisica o un supporto governativo. Vengono scambiate e memorizzate elettronicamente.

La valuta, in qualche forma, è in uso da almeno 3.000 anni. Un tempo solo sotto forma di monete, la moneta si è rivelata fondamentale per facilitare il commercio tra i continenti.

Una caratteristica fondamentale della valuta moderna è che non ha valore in sé. Le banconote, cioè, sono pezzi di carta e non monete d'oro, d'argento o di bronzo.

Il concetto di usare la carta come moneta potrebbe essere stato sviluppato in Cina già nel 1000 a.C., ma l'accettazione di un pezzo di carta in cambio di qualcosa di valore reale ha richiesto molto tempo per prendere piede. Le valute moderne sono emesse su carta in vari tagli, con emissioni frazionarie sotto forma di monete.

Differenze tra Denaro e Valuta Spesso si usano i termini money o denaro e currency o valuta in modo interscambiabile ma, pur essendo correlati, hanno significati diversi.

Denaro è un termine più ampio che si riferisce a un sistema intangibile di valore che rende possibile lo scambio di beni e servizi, oggi e in futuro. Valuta è semplicemente una forma tangibile di denaro.

Il denaro o moneta o anche soldi secondo le scienze economiche è uno strumento che può assumere le funzioni di:

- mezzo di scambio
- unità di conto
- riserva di valore
- riferimento per pagamenti dilazionati

Denaro viene utilizzato in vari modi, tutti legati al suo utilizzo futuro in qualche tipo di transazione. Ad esempio, il denaro è una riserva di valore. Ciò significa che ha e mantiene un certo valore che supporta gli scambi correnti. Le persone presumono che il denaro ricevuto oggi avrà essenzialmente lo stesso valore in un futuro prossimo, quando dovranno fare un acquisto o pagare una bolletta.

Il denaro è anche definito unità di conto. Ciò significa che può essere utilizzato per contabilizzare le variazioni di valore degli oggetti nel tempo. Le aziende utilizzano il denaro come unità di conto quando preparano un bilancio o attribuiscono un valore alle attività. I profitti e le perdite vengono stabiliti e considerati utilizzando il denaro come unità di conto.

Il denaro ha anche alcune proprietà che consentono uno scambio agevole di beni:

- È fungibile, ovvero scambiabile, in modo da non dover essere rivalutato per ogni transazione.
- È durevole, in modo che possa essere utilizzato per fare molti scambi nel tempo.
- È comoda da trasportare e da dividere.

- È riconoscibile, in modo che le persone possano fidarsi e portare a termine con fiducia i loro scambi di beni e servizi.
- L'offerta di moneta deve essere stabile, in modo che il suo valore sia affidabile.

Capire cos'è il denaro chiarisce il significato di Valuta. È una forma di denaro utilizzata quotidianamente dalle persone di tutto il mondo. Gli assegni sono un'altra forma di denaro (noti come sostituti del denaro). Anche le sigarette sono state una forma di denaro, ad esempio per i detenuti nelle prigioni o per i soldati durante la Seconda Guerra Mondiale.

Custodial

Livello: base

Argomento: legale

Con custodial, o custotian, wallet vengono indicati i conti in criptovalute gestite da exchange entralizzati o altri servizio di criptovalute, dei quali l'utente non ha un controllo diretto come succede per i veri wallet Bitcoin.

Essendo infatti nel totale controllo dei custodial, non dovrebbero essere definiti wallet ma semplicemente dei "conti", perché questi assomigliano più ai conti bancari che ai wallet di criptovalute.

Il custodian, il custode, è responsabile di custodire in modo sicuro il denaro dell'utente, l'utente non ha le chiavi private per poter gestire le proprie criptovalute, ma può operare solo mandando richieste alla terza parte custodial che gestirà le richieste secondo le proprie policy.

La terza parte custodial potrebbe non avere neanche tutta la riserva di criptovalute corrispondente ai depositi dei suoi clienti, con notevoli rischi per la solvibilità dei propri conti.

Un wallet custodial è meno sicuro di un wallet non custodial.
Tuttavia, molte persone continuano a sceglierli perché li ritengono più facili da usare e comportano meno responsabilità.
Se gli utenti dimenticano la password del loro conto di scambio, possono probabilmente ripristinarla attraverso i processi di verifica dell'identità.

Questo comporta che la terza parte ha il pieno controllo dei fondi e se il servizio viene compromesso o fallisce, i suoi clienti non saranno in grado di accedere ai loro soldi. Per evidenziare che in questi tipi di wallet non si ha il controllo dei propri fondi si usa il detto Not Your Keys, Not Your Coins.

Poiché una delle caratteristiche principali nel detenere bitcoin è avere la completa sovranità sui propri soldi, conservare bitcoin in un custodial vanifica lo scopo di investire e detenere una valuta digitale decentralizzata che ti consente di essere la banca di te stesso.

I custodial wallet sono anche definiti Hosted Wallet, termine ad esempio utilizzato dal MiCA, il regolamento Europeo sui mercati nelle criptovalute.

Confronto tra Custodial e Non-Custodial

	Custodial	Non-Custodial
Chiavi private	Mantenute dal fornitore	Mantenute dall'utente
KYC	Generalmente richiesto	Non è richiesto
Limiti di prelievo	Sì	Nessun limite
Possibile perdita dei fondi in caso di fallimento	Sì	No
Possibilità di sequestro dei fondi	Sì	No

Cypherpunk

Livello: intermedio

Argomento: politica

Un cypherpunk è attivista libertario che sostiene l'uso diffuso della crittografia avanzata e delle tecnologie che migliorano la privacy come mezzo per il cambiamento sociale e politico.

Comunicando originariamente attraverso la mailing list elettronica Cypherpunks, i gruppi informali miravano a raggiungere la privacy e la sicurezza attraverso l'uso proattivo della crittografia. Le idee e il lavoro dei Cypherpunk sono stati propedeutici alla creazione di Bitcoin.

Il Manifesto Cypherpunk di Eric Hughes recita:

"La privacy è necessaria per una società aperta nell'era elettronica. La privacy non è segretezza. Una questione privata è qualcosa che non si vuole far sapere al mondo intero, ma una questione segreta è qualcosa che non si vuole far sapere a nessuno. La privacy è il potere di rivelare selettivamente se stessi al mondo… Pertanto, la privacy in una società aperta richiede sistemi di transazione anonimi. Finora il contante è stato il sistema principale. Un sistema di transazione anonimo non è un sistema di transazione segreto. Un sistema anonimo consente agli individui di rivelare la propria identità quando lo desiderano e solo quando lo desiderano; questa è l'essenza della privacy".

L'11 febbraio 2009, Satoshi Nakamoto scrisse di una prima versione di Bitcoin su un forum online dei cypherpunk. Sebbene questo non sia il primo annuncio ufficiale del rilascio di Bitcoin, contiene un buon riassunto delle motivazioni di Satoshi.

DAICO

Acronimo di: Decentralized Autonomous Initial Coin Offerings

Livello: avanzato

Argomento: finanza

Un metodo per il finanziamento decentrato di progetti, che combina idee provenienti da organizzazioni autonome decentralizzate (DAO) e offerte iniziali di monete (ICO), proposte da Vitalik Buterin, creatore di Ethereum. Introduce una forma di governance nel processo di ICO, consentendo ai sostenitori di votare per il ritorno dei loro fondi se vengono soddisfatte determinate condizioni.

DAO

Acronimo di: Decentralized Autonomous Organization

Livello: intermedio

Argomento: politica

Questo termine è usato per descrivere un'organizzazione che utilizza la tecnologia blockchain per la propria gestione, come ad esempio smart contracts e registri distribuiti: non necessita quindi di un ente di controllo centrale.

dApps

Acronimo di: Decentralized Application

applicazioni decentralizzate

Livello: intermedio

Argomento: tecnologia

Sono applicazioni che vengono eseguite su un sistema informatico distribuito, ovvero una rete blockchain. Non sono controllate da una singola entità o autorità. Invece, sono gestite da più utenti (o nodi). L'applicazione è protetta dalla crittografia, il che significa che tutti i dati vengono registrati e mantenuti in una blockchain pubblica. Il vantaggio principale di una DApp rispetto a un'app tradizionale è che quest'ultima utilizza un'architettura centralizzata archiviando i propri dati su server controllati da un'unica entità.

Dark Skippy

Livello: avanzato

Argomento: tecnologia

Dark Skippy è un tipo di attacco che consente ad un attaccante malintenzionato, che è riuscito a compromettere il firmware di un hardware wallet, di usare una

funzione di firma modificata per esfiltrare il Seed Phrase della vittima incorporandolo nelle firme delle transazioni.

L'attacco funziona in questo modo:

1. Un aggressore carica un firmware maligno sul tuo wallet hardware.
2. Invii una transazione bitcoin usando questo wallet hardware compromesso. Il firmware maligno incorpora la tua seed phrase codificandola nella transazione, che ora è pubblicamente sulla blockchain.
3. L'attaccante trova la tua transazione sulla blockchain, esegue su di essa un particolare algoritmo (Pollard's kangaroo algorithm) ed estrae la tua seed frase.
4. Grazie al tuo seed, l'attaccante ha ora accesso ai tuoi fondi.

Questo exploit richiede che il signer sia corrotto tramite firmware maligno e non influisce sui wallet hardware che usano multisig tra l'host e il dispositivo di firma. In precedenza si pensava che ci volessero decine di firme/transazioni perché un dispositivo di firma dannoso facesse trapelare un seed segreto a un aggressore, incorporandolo di nascosto nelle firme delle transazioni. Abbiamo dimostrato che è possibile farlo in sole due firme. Un singolo utilizzo di un portafoglio hardware dannoso è sufficiente per perdere tutto.

Innanzitutto, un aggressore deve corrompere un dispositivo di firma: Un dispositivo di firma potrebbe essere manomesso per caricare firmware dannoso. L'utente potrebbe essere indotto con l'inganno a installare firmware dannoso sul proprio dispositivo. L'aggressore potrebbe creare dispositivi dannosi da vendere o infiltrarsi nelle catene di fornitura.

Per contrastare tale vulnerabilità, è disponibile il protocollo Anti-Exfil implementato dagli hardware wallet Jade e BitBox02.

La vulnerabilità si chiama Skippy in riferimento al fatto che viene utilizzato l'algoritmo Pollard's kangaroo, o canguro, e ad una vecchia serie televisiva Skippy il canguro.

Dark Web

Livello: intermedio

Argomento: legale

È quella parte del World Wide Web che esiste sulle Darknet: reti che utilizzano Internet ma richiedono software, configurazioni o autorizzazione specifici per l'accesso. Attraverso il dark web, le reti informatiche private possono comunicare e condurre affari in modo anonimo senza divulgare informazioni identificative, come l'indirizzo ip di un utente e da questo la sua possibile posizione.

Il dark web viene spesso confuso con il Deep Web, ovvero la parte del web non indicizzata dai motori di ricerca e quindi non ricercabile. Il dark web è

una sottosezione più piccola del Deep Web che richiede un software speciale per ospitare e visitare le pagine web.

Per accedere al dark web sono necessarie reti appositamente progettate, come Tor, che fornisce accesso anonimo, e I2P, che consentono l'hosting anonimo di siti web.

La crittografia a strati del dark web, che instrada le comunicazioni attraverso un gran numero di nodi volontari, con ogni nuovo nodo che aggiunge un ulteriore livello di crittografia, offre maggiori garanzie che le identità e le posizioni degli utenti non vengano rivelate a nessuno. Sia i visitatori che gli host delle pagine del dark web non sono in grado di ottenere informazioni personali l'uno sull'altro, consentendo loro di comunicare in totale riservatezza.

Questo livello di privacy non caratteristico dell'Internet normale, o Clearnet come viene chiamato per contrapposizione al Dark web, consente uno scambio di idee e informazioni più privato e quindi libero tra gli utenti.

Storicamente e ancora per molti media, viene associato e il suo uso finalizzato ad attività altamente illegali e immorali sui mercati del dark web, come la vendita di droghe illegali, armi da fuoco e pornografia infantile.

Darknet

Livello: intermedio

Argomento: tecnologia

Con Darknet si intendono i servizi costruiti su Tor o altre reti di anonimato, la cui connessione è criptata e anonimizzata.

Poiché la privacy è un aspetto fondamentale per gli utenti Bitcoin e i gestori di componenti e servizi della rete quali Full node, Lightning Network, l'uso di sistemi di anonimizzazione e quindi della Darknet è sempre più una componente essenziale per il funzionamento della rete Bitcoin.

Al termine Darknet, viene contrapposto il termine Clearnet che indica la rete Internet nel quale il traffico non viene criptato e quindi informazioni quali indirizzi ip e altre informazioni sono esposte a soggetti che potrebbero essere degli attaccanti nel più ampio significato del termine.

La Darknet è quindi sempre meno riferibile all'uso di tecniche di protezione da parte di malfattori, e sempre più una modalità di utilizzo per servizi nei quali la privacy è importante.

Alcuni browser Web, quali Brave Browser, sono abilitati per poter accedere ai siti su Darknet, o Dark Web.

datacarrier

Livello: avanzato

Argomento: tecnologia

Il datacarrier, in italiano trasportatore di dati, si riferisce alla possibilità di inserire dati nelle transazioni Bitcoin, e ai parametri per controllare tale possibilità da parte di un nodo.

La blockchain Bitcoin, ha potenziali utilizzi che vanno oltre i pagamenti.
Molti sviluppatori hanno cercato di utilizzare il linguaggio di scripting delle transazioni per sfruttare la sicurezza e la resilienza di Bitcoin in applicazioni come servizi di notarizzazione digitale, certificati azionari e smart contract.

I primi tentativi di utilizzare il linguaggio di script di Bitcoin per questi scopi prevedevano la creazione di output nelle transazioni che registravano dati sulla blockchain; ad esempio, per registrare un'impronta di un file in modo che chiunque potesse dimostrare l'esistenza di quel file in una data specifica facendo riferimento a quella transazione.

L'uso della blockchain di Bitcoin per archiviare dati non correlati ai pagamenti di Bitcoin è un argomento controverso.
Molti sviluppatori considerano tale uso abusivo e vogliono scoraggiarlo. Altri lo vedono come una dimostrazione delle potenti capacità della tecnologia blockchain e vogliono incoraggiare tale sperimentazione.

Coloro che si oppongono all'inclusione di dati non legati ai pagamenti sostengono che provochi un "gonfiore della blockchain", gravando coloro che gestiscono full node con i costi di archiviazione su disco per dati che la blockchain non era destinata a trasportare. Inoltre, tali transazioni creano UTXO che non possono essere spesi, utilizzando l'indirizzo Bitcoin di destinazione come un campo libero di 20 byte. Poiché l'indirizzo è utilizzato per i dati, non corrisponde a una chiave privata e l'UTXO risultante non può mai essere speso; è un pagamento falso. Queste transazioni che non possono mai essere spese non vengono quindi rimosse dall'UTXO set e causano un aumento continuo delle dimensioni del database UTXO definito bloat.

Nel 2014 con la versione 0.9 di Bitcoin Core, si è raggiunto un compromesso con l'introduzione dell'operatore OP_RETURN, non come sostegno condiviso all'archiviazione di dati nella blockchain, ma con una modifica OP_RETURN che crea un output provabilmente eliminabile, per evitare schemi di archiviazione dati - alcuni dei quali erano già stati implementati - che archiviavano dati arbitrari come immagini in output delle transazioni permanentemente spendibili, gonfiando il database UTXO di bitcoin.
OP_RETURN consente agli sviluppatori di aggiungere qualche decina di byte di dati non legati ai pagamenti a un output di transazione. Tuttavia, a differenza dell'uso di UTXO "falsi", l'operatore OP_RETURN crea un output esplicitamente e provabilmente ineseguibile, che non deve essere archiviato nell'UTXO set. Gli output OP_RETURN vengono registrati sulla blockchain, quindi occupano spazio su disco e contribuiscono all'aumento delle dimensioni della blockchain, ma non vengono archiviati nell'UTXO set e quindi non

gonfiano la memoria pool UTXO e gravano sui full node con i costi maggiori in termini di memoria RAM.

La porzione di dati è limitata e rappresenta più spesso un hash, come l'output dell'algoritmo SHA256 (32 byte). Molte applicazioni aggiungono un prefisso davanti ai dati per aiutare a identificare l'applicazione.

Non esiste uno script di sblocco che potrebbe essere utilizzato per "spendere" un output OP_RETURN, che di solito è un output con un importo di bitcoin pari a zero, perché qualsiasi bitcoin assegnato a tale output è effettivamente perso per sempre.

Se un output OP_RETURN viene indicato come input in una transazione, il motore di validazione dello script interromperà l'esecuzione dello script di validazione e contrassegnerà la transazione come non valida.

Una transazione standard (quella conforme ai controlli IsStandard()) può avere solo un output OP_RETURN. Tuttavia, un singolo output OP_RETURN può essere combinato in una transazione con output di qualsiasi altro tipo.

Nel 2015 a partire dalla versione 0.10 sono state aggiunte due nuove opzioni da riga di comando in Bitcoin Core:

- `datacarrier`: L'opzione datacarrier controlla il relay e il mining delle transazioni RETURN, con il valore predefinito "1" per consentirle.
- `datacarriersize`: L'opzione datacarriersize richiede un argomento numerico che specifica la dimensione massima in byte dello script OP_RETURN (o più precisamente degli scriptPubKey che trasportano dati) e conseguentemente dei dati che possono essere inseriti in un output. il valore di default di 83 byte, che consente un massimo di 80 byte di dati RETURN più un byte dell'opcode RETURN e due byte dell'opcode PUSHDATA.

Questa dimensione impatta le transazioni che vengono distribuite dal nodo alla rete (relay) e per la costruzione del blocco da minare, ma non impatta la validità delle transazioni di un blocco (algoritmo di consenso).

Questa impostazione di default è cambiata nel tempo poiché l'uso di OP_RETURN è stato ed è dibattuto perché incorporare dati nella blockchain di Bitcoin ne aumenta le dimensioni senza supportare direttamente il trasferimento di Bitcoin e per alcuni questo è un uso improprio di Bitcon:

- v0.9.0 40 byte: con Bitcoin Core 0.9.0, il limite di dimensioni di OP_RETURN era impostato a 40 byte
- v0.11 80 byte: nel 2016, con la versione Bitcoin Core 0.11, il limite di dimensioni di OP_RETURN è stato aumentato a 80 byte.

- v0.12 83 byte: dalla versione Bitcoin Core 0.12, le regole di inoltro standard consentono un singolo output con OP_RETURN, che contiene qualsiasi sequenza di istruzioni push (o OP_RESERVED) dopo OP_RETURN

a condizione che sia al massimo 83 byte.

Nel 2023 con l'introduzione Inscription, si ravviva la polemica sull'uso o presunto abuso della blockchain Bitcoin, sul quale debba essere una giusta dimensione.

Luke Dashjr, col dichiarato tentativo di filtrare le Inscription produce una patch per Bitcoin Core chiamata Ordisrespector, che segue quanto aveva già fatto con una versione di Bitcoin Core modificata chiamata Knots, con il parametro `datacarriersize` impostato a 42 byte dal 2016, ed estendendo il controllo di questa dimensione degli extra data nelle transazioni non solo le i dati di OP_RETURN (le Inscription non usano infatti OP_RETURN).

DCA

Acronimo di: Dollar Cost Averaging

Piano d'Accumulo del Capitale

Livello: intermedio

Argomento: finanza

Il DCA, in italiano PAC (Piano d'Accumulo del Capitale) è un piano di risparmio che permette agli investitori di investire importi in modo regolare. Gli investitori possono scegliere di versare regolarmente un importo fisso in PAC o possono scegliere di investire una percentuale dei loro redditi, indipendentemente dal prezzo del titolo acquistato. È una strategia di investimento in cui un investitore divide il suo capitale di investimento per fare acquisti periodici di un'attività per ottenere un miglior prezzo medio complessivo di ingresso. Il DCA è spesso considerato una delle strategie di investimento più prudenti per le criptovalute a causa della volatilità intrinseca del settore. La DCA aiuta gli investitori ad evitare acquisti di grandi somme in un momento sbagliato. Un esempio di DCA potrebbe essere quella dove un investitore che compra $100 USD di bitcoin (BTC) ogni settimana per un lungo periodo di tempo, a prescindere da quale sia il prezzo del BTC al momento dell'acquisto.

DDoS

Acronimo di: Distributed Denial of Service

Livello: avanzato

Argomento: tecnologia

L'attacco DDoS, Distributed Denial of Service, è un tipo di attacco informatico DoS tramite il quale l'attaccante travolge il sistema attaccato con una grande quantità di richieste provenienti da molti computer distribuiti in rete, sovraccaricandolo al punto tale da impedirgli di soddisfare le richieste legittime.

Questi computer dai quali parte l'attacco spesso sono parte di una Botnet, una rete composta da dispositivi infettati da malware, detti bot o zombie, che agiscono tutti sotto lo stesso controllo di un unico dispositivo di un attaccante.

Dead Cat Bounce

Livello: avanzato

Argomento: finanza

Il Dead Cat Bounce (letteralmente il rimbalzo del gatto morto, ma anche in Italia viene usato il termine inglese) è una temporanea ripresa dei prezzi dopo un calo prolungato, un breve recupero del prezzo di un asset in calo che è subito seguito da una continuazione del trend ribassista.

Un dead cat bounce è un pattern nel grafico dei prezzi nell'analisi tecnica. Si verifica in attività che sono in una tendenza al ribasso di lungo termine e rappresenta una breve ripresa, seguita da un ritorno al minimo precedente e da un continuo movimento al ribasso.

Un dead cat bounce è più specificamente un pattern di mercato o il comportamento di una criptovaluta, un'azione, o qualsiasi altra risorsa che mostra una ripresa a breve termine in mezzo a una tendenza al ribasso. Può essere un movimento al rialzo di breve durata di un'attività dopo una correzione importante o un movimento al ribasso.

Questo termine deriva da un modo di dire di Wall Street che recita: "*anche un gatto morto rimbalzerà se cade da una grande altezza*".

Può verificarsi quando un numero sufficientemente elevato di trader ribassisti chiude le proprie operazioni short avviate in precedenza o quando un numero altrettanto significativo di investitori rialzisti ritiene che un asset abbia toccato il fondo e inizia ad aprire operazioni long su di esso.

Un dead cat bounce è un pattern di continuazione, ovvero dopo che si è verificato, il prezzo continua a muoversi nella direzione prevalente a lungo termine. Il pericolo di questo pattern è che all'inizio potrebbe apparire come un'inversione della tendenza generale di un asset, portando i trader e gli investitori rialzisti ad andare long su di esso solo perché il prezzo continui a scendere in seguito.

Tuttavia, il picco di questo fenomeno presenta anche un'opportunità per i trader di avviare operazioni short con l'intenzione di trarre profitto quando l'attività riprenderà la sua caduta.

Sebbene esistano alcuni metodi di analisi tecnica e fondamentale che consentono di provare a prevedere se la ripresa sia solo temporanea, si tratta di un compito complesso con risultati inaffidabili. In quanto tali, possono essere chiamati definitivamente solo dopo aver terminato il loro corso.

Esistono molteplici variabili che potrebbero indicare la causa di un dead cat bounce, ad esempio quando i ribassisti iniziano a chiudere le loro posizioni short

o quando i rialzisti iniziano ad aprire nuove posizioni lunghe credendo che un asset abbia già toccato il fondo. Ci sono anche casi in cui i trader di momentum iniziano ad accumulare posizioni non appena vedono l'indice di forza relativa di un asset a livelli di ipervenduto.

Sfortunatamente, molti trader alle prime armi, specialmente nel settore delle criptovalute, cadono preda dei dead cat bounce poiché credono che gli asset che acquistano siano sulla buona strada per il recupero. Ciò è esacerbato dalla mancanza di regolamentazione del settore delle criptovalute, che aiuta a facilitare attività losche come il front-running e la manipolazione dei prezzi.

Pertanto, è importante che gli analisti osservino ulteriormente il mercato ogni volta che un asset si muove improvvisamente in una tendenza al rialzo dopo un calo continuo poiché non indica sempre un'inversione rialzista, ma potrebbe anche essere un dead cat bounce, che probabilmente non recupererà per un po' i massimi precedenti.

È sempre necessario ricordare che questi capovolgimenti non riflettono in realtà il valore effettivo di qualsiasi attività finanziaria, ma riflettono la psicologia collettiva del mercato, che è caotica e in continua evoluzione. Le misure precauzionali dovrebbero essere osservate prima che i trader aprano nuove posizioni in qualsiasi circostanza.

Debasement

Svilimento della moneta

Livello: avanzato

Argomento: politica

Il debasement è la deliberata riduzione del valore di una valuta. Per commodity come le monete d'oro o d'argento, il debasement si ottiene solitamente attraverso una riduzione del contenuto d'oro o d'argento di una moneta. Per la moneta digitale o cartacea, il debasement può essere ottenuta semplicemente creando più denaro. Il debasement viene solitamente attuato dai governi per finanziare i loro sforzi a spese dei loro cittadini.

Il debasement è un'alternativa alla tassazione diretta ed è meno ovvia per la maggior parte dei cittadini. Per questi motivi, i governi dall'Impero Romano agli Stati Uniti hanno fatto il debasement della loro valuta. Nel 1965, il governo degli Stati Uniti ridusse il contenuto d'argento del mezzo dollaro d'argento dal 90% al 40% mentre legiferava che entrambe le monete valessero lo stesso importo. In questo caso e in molti altri, lo svilimento ha innescato gli effetti della legge di Gresham.

Il debasement si è avuto anche a seguito della fine del gold standard: si passò lentamente da un'economia mondiale che utilizzava l'oro come moneta a un'economia in cui i certificati cartacei venivano emessi come credito su quell'oro. Addirittura, la carta è stata completamente separata da qualsiasi

supporto fisico da Nixon, che ha posto fine alla convertibilità internazionale del dollaro USA in oro nel 1971.
La fine del gold standard permise ai governi e alle banche centrali di aumentare a piacimento l'offerta di moneta, diluendo il valore di ogni banconota in circolazione, il debasement. Sebbene la moneta fiat pura, emessa dai governi e riscattabile in cambio di nulla, sia il denaro che tutti conosciamo e utilizziamo quotidianamente, si tratta in realtà di un esperimento relativamente nuovo nell'ambito della storia mondiale.

Si dovrebbe avere fiducia che i nostri governi non abusino della loro possibilità di stampare denaro, ma non dobbiamo cercare lontano per trovare esempi di violazione di questa fiducia. Nei regimi autocratici e pianificati centralmente, dove il governo ha il dito direttamente sulla macchina del denaro, come il Venezuela, la moneta è diventata quasi priva di valore.

Per evitare il debasement, Satoshi Nakamoto con Bitcoin ha progettato un sistema monetario in cui l'offerta è fissa ed emessa a un tasso prevedibile e immutabile. Il max supply, o offerta massima, di Bitcoin sarà 21 milioni, ci saranno solo 21 milioni di bitcoin, anche se ogni bitcoin può essere diviso in 100 milioni di unità, ora chiamate satoshi, per un totale finale di 2,1 quadrilioni di satoshi in circolazione intorno all'anno 2140.

decentralized

decentralizzato

Livello: base

Argomento: tecnologia

Un sistema decentralizzato è caratterizzato dalla distribuzione dell'autorità decisionale e del controllo su più entità o nodi autonomi. In un sistema decentralizzato, nessun ente o nodo centrale detiene il potere decisionale o il controllo completo.

Le decisioni e le operazioni vengono prese in modo distribuito tra le diverse entità all'interno del sistema. Questo approccio mira a ridurre la dipendenza e l'influenza di un'autorità centrale, offrendo maggiore autonomia e resistenza a eventuali guasti o attacchi. Un esempio di sistema decentralizzato è una blockchain, in cui le transazioni vengono validate e registrate da una rete di nodi distribuiti.

Spesso quando si confrontano sistemi o reti in relazione alla loro centralizzazione, viene fatto riferimento ai modelli descritti da Paul Baran che li distingue in:

- centralizzati,
- decentralizzati,
- e distributi.

La differenza tra “decentralizzato” e “distribuito” riguarda principalmente la struttura e l’organizzazione di un sistema o di una rete.
Distribuito può indicare che il calcolo è distribuito su più nodi anziché su uno solo, decentralizzato che nessun nodo sta impartendo istruzioni ad altri nodi su cosa fare.

Mentre un sistema basato su blockchain è intrinsecamente distribuito (il che significa che molte parti hanno copie del registro), non è intrinsecamente decentralizzato.
Se sia centralizzato o decentralizzato può riferirsi ai diritti dei partecipanti sul registro ed è quindi una questione di progettazione.

Poiché il ledger di Bitcoin, il libro mastro, non si trova più in un unico luogo, lo chiamiamo distribuito e, poiché non c’è una parte centrale che se ne occupa, lo chiamiamo decentralizzato. In questo modo si risolve il problema dell’eliminazione dell’intermediario.

In sintesi, la decentralizzazione si riferisce alla distribuzione del potere decisionale e del controllo, mentre la distribuzione si riferisce alla suddivisione delle risorse o delle funzionalità su più nodi o dispositivi.

Tuttavia, è importante notare che i concetti di decentralizzazione e distribuzione possono essere interconnessi e spesso coesistono in vari sistemi e reti complessi.

Bitcoin è sia distribuito che decentralizzato. La rete di Bitcoin è distribuita perché le transazioni e i dati associati sono archiviati su molti nodi nella rete, chiamati full node (nodi completi). Ogni full node ha una copia dell’intera blockchain di Bitcoin e partecipa al processo di convalida e propagazione delle transazioni.

Allo stesso tempo, Bitcoin è anche decentralizzato perché non esiste un’autorità centrale che controlli o gestisca la rete. Le decisioni riguardanti il funzionamento del protocollo e la validazione delle transazioni sono prese da un consenso tra i partecipanti alla rete. Non c’è un singolo nodo o entità che possa impartire istruzioni agli altri nodi o prendere decisioni unilaterali.

La combinazione di distribuzione e decentralizzazione fa sì che Bitcoin sia resiliente, sicuro e resistente alla censura. Ogni nodo completo ha una copia indipendente della blockchain e partecipa alla verifica delle transazioni, garantendo che la rete continui a funzionare anche in presenza di guasti o attacchi mirati a un singolo nodo o gruppo di nodi.

decoy wallet

portafoglio esca

Livello: base

Argomento: tecnologia

Un decoy wallet, portafoglio esca in italiano, è un wallet creato per ingannare potenziali ladri. Questo wallet è progettato per sembrare un wallet principale reale e può contenere una piccola quantità di Bitcoin, ma non custodisce la maggior parte delle tue risorse. Viene utilizzato insieme ad altre misure di sicurezza, come l'autenticazione a due fattori, per fornire un ulteriore livello di protezione.

Sebbene non sia una misura di sicurezza rivoluzionaria, il decoy wallet può essere utile per chi vuole migliorare la propria sicurezza in ambito cripto. Lo scopo principale è ingannare i ladri, facendoli credere di aver trovato il tuo wallet principale, mentre in realtà stanno accedendo solo a una porzione ridotta delle tue criptovalute.

Perché usare un decoy wallet?

Creando un decoy wallet, puoi far credere ai ladri di aver ottenuto l'accesso alle tue criptovalute. Anche se il contenuto è effettivamente tuo, non avranno accesso alla maggior parte delle tue risorse. Questo può scoraggiare ulteriori tentativi di furto. Inoltre, se un hacker dovesse accedere al tuo dispositivo, potrebbe individuare il decoy wallet e non cercare il vero wallet con la maggior parte delle tue criptovalute.

L'uso di un decoy wallet non diminuisce la probabilità che un ladro trovi un tuo wallet, ma aumenta lo sforzo necessario per accedere a tutti i tuoi beni. Questo può far sì che i ladri impieghino più tempo e risorse, aumentando le possibilità di essere scoperti o di rinunciare al furto.

Un altro vantaggio è che, se un ladro accede al decoy wallet, potrebbe smettere di cercare il tuo wallet principale, permettendoti di prendere ulteriori misure di sicurezza, come cambiare password o attivare l'autenticazione a due fattori.

Come utilizzare un decoy wallet Per creare un decoy wallet, dovrai generare un nuovo indirizzo e trasferirci una piccola quantità di criptovalute. Ecco alcuni consigli:

Non effettuare transazioni tra il decoy wallet e quello principale, per evitare tracce evidenti. Usa un nome credibile per il decoy wallet.
Assicurati che il decoy wallet abbia qualche attività, come piccole transazioni, per farlo sembrare autentico.
Non sacrificare le misure di sicurezza del decoy wallet, per non destare sospetti.
Usa un software o hardware diverso per il decoy wallet e proteggilo con password o PIN unici e forti. Mantieni il decoy wallet attivo con piccole transazioni periodiche.
Ricorda che il decoy wallet non è un backup, ma solo una trappola: le risorse contenute devono essere sacrificabili.

Come agiscono i ladri? La maggior parte dei ladri di criptovalute non cerca specificamente portafogli mirati, ma usa strumenti automatizzati per scansion-

are la blockchain alla ricerca di vulnerabilità, come portafogli non protetti o con password deboli. Una volta individuato un wallet vulnerabile, i ladri possono usare metodi come attacchi di ingegneria sociale, phishing o malware per ottenere l'accesso.

In definitiva, l'obiettivo di un decoy wallet è aggiungere un ulteriore livello di protezione per i tuoi beni. Creando un wallet realistico con una piccola quantità di criptovalute, puoi ingannare i potenziali ladri, riducendo le probabilità che tentino di rubare il tuo vero wallet.

Deep Web

Livello: intermedio

Argomento: tecnologia

Il Deep Web, in italiano Web sommerso, Web invisibile o Web nascosto, e qualla parte del World Wide Web i cui contenuti non sono indicizzati dai motori di ricerca web standard, e quindi non è facilmente accessibile attraverso i loro risultati di ricerca.

Il Deep Web include molti siti web che sono privati o protetti da password, nonché pagine all'interno di siti web che non sono pubblicamente accessibili.

Si contrappone al Surface web, chiamato anche Web visibile, Web indicizzato, Web indicizzabile, che è direttamente disponibile al pubblico e ricercabile con i motori di ricerca web standard.

Il Deep Web è spesso confuso con il Dark Web, che è una sottosezione del Deep Web che è accessibile solo tramite software speciali, come TOR.

DeFi

Acronimo di: Decentralized Finance

finanza decentralizzata

Livello: intermedio

Argomento: finanza

Si riferisce all'ecosistema composto da applicazioni finanziarie che vengono sviluppate su sistemi blockchain. DeFi può essere definito come il movimento che promuove l'uso di reti decentralizzate e software open source per creare molteplici tipi di servizi e prodotti finanziari. L'idea è di sviluppare e gestire DApp finanziarie su un framework trasparente e affidabile, come blockchain, senza autorizzazione e altri protocolli peer-to-peer (P2P)

Deflation

Deflazione

Livello: intermedio

Argomento: politica

La deflazione è una diminuzione generalizzata dei prezzi di beni e servizi.

La deflazione è l'opposto dell'inflazione e si riferisce alla graduale riduzione dei prezzi in un'economia rispetto al valore reale, che aumenta il potere d'acquisto di una valuta nel tempo. La deflazione di solito accompagna la contrazione dell'offerta monetaria in una data economia, mentre l'inflazione è spesso il risultato di una maggiore stampa di denaro. I Bitcoin generalmente vengono considerati avere una natura deflazionistica, poiche l'emissione delle nuove monete stabilita nel suo protocollo riduce l'offerta circolante di bitcoin nel tempo attraverso una operazione definita Halving.

La deflazione è una diminuzione generale del prezzo di beni e servizi in un'economia nel tempo. Questo si traduce in un maggiore potere d'acquisto per la relativa valuta. La deflazione è rara nelle economie moderne e si verifica più spesso durante le recessioni. La deflazione a breve termine può avere effetti diversi sull'economia. La deflazione a lungo termine è generalmente negativa per un'economia. La deflazione è l'opposto dell'inflazione.

La deflazione è generalmente misurata in base ai prezzi di beni e servizi. I prezzi di questi prodotti sono tracciati da un paniere di mercato medio ponderato di molte voci, noto come indice dei prezzi al consumo (CPI).

Ci sono diversi possibili fattori di deflazione. Se l'offerta di denaro diminuisce, allora il valore di una valuta salirà, il che abbasserà i prezzi. In alternativa, un improvviso aumento dell'offerta di beni e servizi causerà un prezzo di equilibrio più basso, anche se il valore della valuta è rimasto invariato.

Un prezzo di equilibrio più basso si verificherà anche quando la domanda di beni e servizi scende, come è avvenuto nelle prime fasi della crisi COVID-19. Indipendentemente dal valore della valuta, una minore domanda costringerà i commercianti ad abbassare i prezzi per rimanere competitivi, con conseguente deflazione.

degen

Livello: base

Argomento: finanza

Il termine **degen** è l'abbreviazione di **degenerato** e viene comunemente associato alla DeFi.

Sebbene la finanza decentralizzata rappresenti un'evoluzione dell'ecosistema delle criptovalute, è importante riconoscere che essa comprende anche progetti

al limite della legalità o dell'etica.
Questi progetti sono ciò che costituisce la sottocultura conosciuta come "DeFi degens".

Il termine viene utilizzato in due contesti distinti, che riflettono due facce della stessa medaglia. Da un lato, ci sono piattaforme DeFi discutibili o token "degenerati", spesso associati alla pratica del pump and dump.
Dall'altro lato, ci sono individui desiderosi di acquistare l'ultima criptovaluta con nomi improbabili o che cercano costantemente rendimenti elevati su farm esotiche, inserendo liquidità in pool senza una reale motivazione.

In sostanza, un "degen" è un giocatore d'azzardo, uno scommettitore, e non può essere considerato né un trader né tanto meno un hodler.

Delegation

Delega

Livello: avanzato

Argomento: tecnologia

Un tipo di utente che all'interno delle blockchain Proof of Stake è un delegator (delegato). Questo tipo di utenti sono in grado di prendere tutti o parte dei loro token e di bloccarli temporaneamente per consegnarli a un validatore con l'obiettivo di aumentare il suo stake . Questa azione si definisce delega.

Delisting

Livello: intermedio

Argomento: finanza

Il processo di rimozione di un asset/azione/criptovaluta da un exchange è chiamato delisting, in italiano può essere reso con Delistato.

Quando un progetto non soddisfa più gli standard di quotazione dell'exchange, può essere delistato. Le ragioni del delisting possono essere molteplici, alcune delle quali sono:

- Mancanza di attività di trading regolare;
- Assenza di sviluppo del protocollo
- Affidabilità del network o dello smart contract non soddisfacente;
- Interazione business-to-customer inesistente;
- Prova di attività fraudolente o pericolose;

Un titolo o asset non può più essere acquistato o venduto in un exchange dopo essere stata delistato. Il delisting è in genere permanente, ma l'asset di un progetto può essere reinserito nel listino in circostanze eccezionali. Se un'azienda viene acquistata o diventa privata, può essere delistata volontariamente. Quando

un'azienda non soddisfa gli standard di quotazione stabiliti dagli exchange nei quali sono negoziati i suoi asset, viene delistata involontariamente.

I requisiti per la quotazione possono essere complessi e i vari tipi di emittenti e di titoli possono avere regolamenti specifici. In generale, essi comprendono il deposito tempestivo dei bilanci, un prezzo delle azioni superiore a una certa soglia, un numero ragionevole di azionisti, una soglia minima di capitalizzazione di mercato o requisiti specifici relativi a ricavi, profitti, flussi di cassa e attività di trading. Il delisting può avere serie implicazioni, in quanto le azioni di una società che non sono quotate nelle borse valori più diffuse sono più difficili da esplorare e acquistare per gli investitori. Ciò significa che l'azienda non sarà in grado di offrire nuove azioni al mercato per finanziare le sue nuove iniziative commerciali. Un'imminente bancarotta, l'incapacità di completare le relazioni obbligatorie o un valore delle azioni inferiore alla soglia minima stabilita dall'exchange sono tutte cause possibili per il delisting di un titolo. L'azienda può chiedere di essere reinserita nel listino dopo aver risolto il problema e soddisfatto i criteri di quotazione. Gli investitori hanno spesso sentimenti contrastanti riguardo alla riquotazione di un'azienda, che potrebbe avere un successo limitato durante il suo secondo mandato sul mercato. Anche se non tutte le aziende vengono cancellate dal listino per motivi negativi, ciò protegge i mercati dall'essere inondati da titoli di qualità inferiore provenienti da emittenti che potrebbero essere vicini alla fine del loro ciclo di vita. Le borse contribuiscono a ridurre il rischio sistemico associato al mercato e a salvaguardare gli investitori garantendo che tutti gli emittenti aderiscano a rigorosi requisiti amministrativi.

Nel mondo delle criptovalute, quando un token/coin viene delistato, tutte le sue coppie di trading vengono rimosse dall'exchange delle criptovalute. Tuttavia, agli investitori che hanno già investito nel progetto delistato viene concesso un periodo di tempo specifico per ritirare i propri fondi, dopodiché il progetto di criptovaluta non è più disponibile in alcuna forma sul'exchange' delle criptovalute.

Derivation Path

Percorso di derivazione

Livello: intermedio

Argomento: tecnologia

Il Derivation Path, o percorso di derivazione, è una sequenza di valori utilizzata dai Wallet HD per descrivere la creazione delle diverse chiavi partendo dal seed o dalla Master Key.

La derivazione delle chiavi effettuata dai wallet HD (Hierarchical Deterministic) *inventata* nel 2012 da Pieter Wuille con il BIP32 può essere fatta in molti modi, e si è evoluta nel corso del tempo al punto che il derivation path specificato nel BIP32, composto da una sequenza di campi separati da una barra (slash) del tipo m/0'/0/0 è ormai considerato deprecato.

Man mano che si sono generati nuovi tipi di indirizzi (per non parlare di altre criptovalute), i wallet si sono evoluti e nonostante siano stati fatti grandi progressi in termini di interoperabilità e per il ripristino, gli sviluppatori di wallet continuano a costruire wallet che:

- non implementano gli standard BIP
- implementano uno o più standard BIP, ma in modo incoerente rispetto ad altri portafogli
- implementano uno standard BIP, ma che non è stato ampiamente adottato
- o addirittura creano un sistema usato solo da loro, vedi il caso di Electrum
- non hanno una documentazione chiara sui loro derivation path e sui processi di backup e ripristino

Il Derivation Path viene rappresentato come una stringa di questo tipo:

- **legacy**:
  - `m/i/0/0` basato sull'esempio nel BIP32, non è più utilizzato e non ci sono hardware wallet moderni che lo supportano nativamente. Software come Bitcoin Core possono supportarlo ma non lo utilizzano di default
  - `m/0'/0'` o `m/0'/X'` dove la X viene sostituita da 0 per il primo account, 1 per il secondo e così via
  - `m/44/0'/0'` o `m/44/0'/X'` dove la X viene sostituita da 0 per il primo account, 1 per il secondo e così via
- **standard parziale**: `m/84'/0'/0'` utilizzato per la generazione degli indirizzi. È necessario conoscerlo, insieme alla xpriv, per poter generare gli indirizzi del proprio wallet
- **standard completo**: `m/84'/0'/0'/0/0` rappresenta uno specifico indirizzo. Ogni singolo indirizzo generato (o meglio derivato dalla chiave hd) dal wallet hd, ha questo formato e l'ultima cifra rappresenta il progressivo dell'indirizzo generato. Ad esempio `m/84'/0'/0'/0/3` è il quarto indirizzo nella propria lista

inizialmente descritta nel BIP44.

I campi della sequenza hanno un ruolo per specificare come vengono generate le diverse chiavi private.

Purtroppo le diverse implementazioni effettuate dagli sviluppatori di wallet non seguono le stesse modalità, nel corso del tempo sono nati degli standard che non sono adottati allo stesso modo dai produttori di wallet, e questo fa in modo che non sempre sia semplice o addirittura possibile ripristinare un back up da un wallet ad uno di un altro sviluppatore.

Anche i wallet che fanno riferimento al BIP44 possono aver interpretato l'implementazione in modo inconsistente.

I campi della sequenza sono i seguenti:

m / purpose' / coin_type' / account' / change / address_index

- **m**: è la lettera iniziale che indica il tipo di master key. La lettera m minuscola indica master extended private key, o xprv, e la M maiuscola per i derivation paths per la xpub, la master extended public key.
- **Purpose**, Scopo: Questo campo, che è stato aggiunto con il BIP43, indica quale standard di derivazione viene utilizzato. Le possibilità possono essere:
  - 0 ormai deprecata, è la specifica del percorso di derivazione originale specificata nel BIP 32
  - 44 che si riferiscono agli indirizzi BIP44 P2PKH, gli indirizzi legacy che iniziano con '1'
  - 49 riferito a BIP49 P2WPKH-nested-in-P2SH / indirizzi SegWit che iniziano con '3'
  - 84 riferito a BIP84 P2WPKH / indirizzi SegWit nativi che iniziano con 'bc1'.
  - 86 riferito a BIP86 P2TR / indirizzi Taproot
  - 45 che si riferiscono ai wallet multi-party multi-signature BIP45 P2SH (proposta)
  - 47 che si riferiscono ai codici di pagamento riutilizzabili del BIP47,
  - 48 riferito ai wallet hardware a firma multipla

Alcuni wallet ne supportano più di uno. Ad esempio, molti wallet ora hanno sia il tipo di indirizzo legacy che quello wrapped o nativo SegWit.

- **Coin Type**, Tipo di moneta: il derivation type può essere utilizzato su bitcoin e altre criptovalute. Questo campo indica il tipo di criptovaluta, sulla base di un indice. Ad esempio lo 0 indica Bitcoin, 1 testnet, 60 Ethereum (ETH). Vedi la lista dei tipi di Coin Type su SLIP-0044 : Registered coin types for BIP-0044
  Notare che il BIP45 indica invece questo livello come "Cosigner Index", l'indice della parte che crea un indirizzo multisig P2SH.
- **Account**, Conto: Questo campo, in un wallet multi-account, indica l'identità o la collezione di indirizzi, che consente agli utenti di tenere conti separati per scopi diversi (es. risparmi, donazioni). Notare che il BIP45 non include questo campo. Il BIP47 attribuisce questo livello alla funzione di "Identità" che si può considerare equivalente a "Conto".
- **Change**: 0 per Receive, 1 per Change. Questo campo, se è presente la costante 0, indica gli indirizzi "external chain" (regolari); se la costante 1, indica gli indirizzi "internal chain" o Change. Si noti che il BIP47 indicava questo livello per notification key e i codici di pagamento ephemeral.
- **Address Index**, Indice indirizzo: Questo campo indica il numero di indirizzo specifico in una sequenza, all'interno di un conto.

Notare che i campi "account" e "address_index" iniziano con zero (0). Analogamente a quanto succede nei linguaggi di programmazione nei quali il primo elemento di un array ha 0 come indice.

Esempio pratico: Un utente ha un wallet bitcoin conforme a BIP44 e vuole individuare il secondo indirizzo nel suo terzo account. Il derivation path per il secondo indirizzo di nel terzo conto sarebbe il seguente: `m/44'/0'/2'/1/1`

Un altro elemento di confusione può verificarsi quando i wallet utilizzano lo stesso derivation path per diversi tipi di script. Soprattutto se si utilizzano tipi di script più nuovi o innovativi, i wallet che hanno destinato tali percorsi ad altri script possono causare errori durante l'importazione.

Derive

Derivare

Livello: avanzato

Argomento: tecnologia

Derivare qualcosa significa ottenerlo da una fonte originale. Nel contesto delle cripto, si parla di portafogli e account "derivati" da frasi seme (seed)/frasi di recupero segrete.

Deterministic wallets

Wallet deterministici

Livello: intermedio

Argomento: tecnologia

I Deterministic wallet, o Wallet deterministici, sono dei wallet che consentono la creazione di diversi indirizzi nello stesso wallet, partendo da un unico seed o seme.

In questi wallet è possibile effettuare il backup una volta, anche prima di generare tutti gli indirizzi, perché tutti gli indirizzi futuri sono determinabili in anticipo. Questo è possibile perché per la generazione delle nuove chiavi è deterministica, utilizzando un algoritmo specifico a partire da un singolo seme.

Esistono due diverse forme:

- Sequential Deterministic, nei quali il seed è una passphrase o una sequenza di caratteri che può essere ripetutamente incrementata per generare nuove chiavi private
- Hierarchical Deterministic o HD Wallet introdotti con il BIP32

DEX

Acronimo di: Decentralized Exchange

Exchange decentralizzato

Livello: base

Argomento: finanza

È un tipo di exchange di criptovalute che consente transazioni peer-to-peer dirette online in modo sicuro e senza la necessità di un intermediario. Nessuno ha il controllo su un DEX, e compratori e venditori trattano reciprocamente, su base uno a uno, tramite applicazioni di trading peer-peer (P2P). Un DEX può essere immaginato come una soluzione di trading fai-da-te. Tramite questo sistema è possibile fare trading direttamente dal proprio wallet. Il più grande vantaggio di questo sistema è che i propri fondi non saranno mai affidati ad una società commerciale o ad altre terze parti, ma totalmente gestiti dai proprietari stessi.

DFCA

Acronimo di: Dual Funded Channel Agreements

Livello: avanzato

Argomento: tecnologia

DFCA, Dual Funded Channel Agreements chiamati anche Dual Swaps, sono degli accordi per la creazione di DFC o Dual Funded Channel.

Si tratta di speciali "swaps" che vengono creati tra due parti e che coinvolgono un solo canale.

DHKE

Acronimo di: Diffie–Hellman Key Exchange

Livello: avanzato

Argomento: tecnologia

Nella rete Lightning viene utilizzato il metodo Elliptic Curve Diffie-Hellman (ECDH)).

Si tratta di un protocollo di accordo su chiave anonima che consente a due parti, ciascuna dotata di una coppia di chiavi pubbliche e private a curva ellittica, di stabilire un segreto condiviso su un canale di comunicazione non sicuro. Questo segreto condiviso può essere usato direttamente come chiave o per ricavare un'altra chiave. La chiave, o la chiave derivata, può quindi essere utilizzata per crittografare le comunicazioni successive utilizzando un cifrario a chiave simmetrica. Un esempio di chiave derivata è il segreto condiviso tra la chiave di sessione effimera di un mittente di un onion e la chiave pubblica del nodo di un hop onion, come descritto e utilizzato dal formato SPHINX Mix.

Difficulty

Difficoltà

Livello: base

Argomento: tecnologia

La Difficulty o difficoltà indica quanto sia difficile per i miner creare un nuovo blocco. Questa difficoltà è stabilità per i miner impostando un target hash, è un numero condiviso da tutti i client Bitcoin che i miner dovranno utizzare per la creazione dei nuovi blocchi e la loro aggiunta alla block chain.

Bitcoin è progettato per avere un nuovo blocco aggiunto approssimativamente ogni 10 minuti. Tuttavia, come previsto nel white paper Bitcoin, la velocità con cui vengono risolti i calcoli per validare il blocco posso variare, ad esempio a causa dei progressi nell'hardware utilizzato i miner saranno in grado di effettuare un maggior numero di calcoli

La difficulty viene regolata in modo programmatico ogni 2.016 blocchi in modo che i blocchi Bitcoin vengano convalidati, ovvero aggiunti alla block chain, il più possibile in media ogni 10 minuti.

La rete Bitcoin ha una Difficulty globale.

Poiché un nuovo blocco viene aggiunto alla catena Bitcoin in media ogni 10 minuti circa, ciò significa che questa regolazione dovrebbe avvenire approssimativamente ogni due settimane (2016 blocchi * 10 minuti/blocco = 20.160 minuti, che sono circa 14 giorni).

La difficulty con cui è stato minato un blocco viene memorizzata attraverso un apposito metadato nel Block header.

La difficulty iniziale dei Bitcoin era 1, ed è rimasta tale per circa un anno.

Come viene calcolata la Difficulty di mining di Bitcoin? La difficoltà di mining di Bitcoin viene calcolata con varie formule. Tuttavia, la più comune è:

```
Difficulty Level = Difficulty Target/Current Target
```

Nota che il Difficulty Target è una notazione esadecimale del target hash la cui difficoltà di mining è 1.

Al contrario, il Current Target, o target corrente, è il target hash del blocco di transazioni più recente. Quando i due valori vengono divisi, si ottiene un numero intero che è il livello di difficoltà di mining di Bitcoin.

Ad esempio, se il risultato è di 24 trilioni, allora ci si aspetta che un miner generi circa 24 trilioni di hash prima di poter trovare l'hash vincente. Naturalmente, a volte i miner possono avere fortuna e trovarlo con un numero significativamente inferiore di tentativi.

Come viene regolata la Difficulty di mining di Bitcoin Gli adeguamenti della difficoltà di mining vengono effettuati confrontando il tempo standard necessario per trovare 2.016 blocchi di transazioni sulla rete Bitcoin con il tempo impiegato per trovare gli ultimi 2.016 blocchi.

La rete calcola il tempo totale necessario per estrarre gli ultimi 2.016 blocchi. Il rapporto tra i 20.160 minuti standard (10 minuti x 2.016 blocchi) e il tempo necessario per scalare l'ultima Difficulty Epoch viene quindi moltiplicato dal livello di difficoltà più recente. Il calcolo produce un risultato che determinerà la percentuale di variazione richiesta nella difficoltà di mining che porterà il tempo di blocco ai desiderati 10 minuti.

Tuttavia, un errore nel protocollo Bitcoin originale rende gli adeguamenti del livello di difficoltà basati sui precedenti 2.015 blocchi invece dei teorizzati 2.016 blocchi.

Sebbene l'obiettivo sia un tempo di blocco di 10 minuti, la difficoltà di mining non può essere modificata al di sopra o al di sotto di quattro volte il livello di difficoltà attuale. Il limite superiore per ogni Difficulty Epoch è una variazione del +300%, mentre il limite inferiore è una variazione del -75%. Questa regola è stata messa in atto per eliminare qualsiasi cambiamento brusco nella difficoltà di mining.

Difficulty Adjustment

Livello: intermedio

Argomento: tecnologia

La Difficulty Adjustment, o regolazione della difficoltà o retarget, è una correzione della difficoltà per il mining bitcoin, finalizzata a garantire che la difficoltà cambi in funzione dell'Hash Rate, ovvero la potenza di calcolo utilizzata dai miner, in modo che in media venga minato un bitcoin ogni 10 minuti.

L'algoritmo utilizzato viene chiamato **DAA**, difficulty adjustment algorithm.
La difficoltà viene regolata regolarmente in modo da mirare a un intervallo di blocco medio di 10 minuti, ma non tutti gli intervalli di blocco sono esattamente di 10 minuti.
La distribuzione dei blocchi nel tempo segue un processo statistico noto come processo di Poisson, secondo la quale eventi casuali si verificano con la stessa probabilità in ogni intervallo di tempo.

Di solito, l'Hash rate aumenta: si aggiungono nuovi miner alla rete Bitcoin, e vengono immessi sul mercato hardware di mining con maggiore potenza di calcolo. Questo fa in modo che i blocchi vengano minati più velocemente.

Ci sono anche dei casi nei quali l'Hash rate diminuisce: ad esempio nel 2021 i miner cinesi per motivi normativi hanno dovuto interrompere o spostare le loro attività, causando una forte diminuzione dell'Hash rate. Un altro motivo per la diminuzione dell'Hash rate può essere dovuto ad un Bear market o Crypto

winter che rende meno profittevole il mining fino a compromettere i bilanci dei miner costringendoli a spegnere le loro macchine o addirittura a chiudere, ma in questo periodo nonostante qualcuno lo definisca come Bear market siamo vicino ai massimi.

L'aggiustamento della difficoltà anche se cerca di impostare un tempo medio di 10 minuti, non è però in condizioni di garantire tale tempo, e quindi tra un blocco il successivo possono passare pochi secondi o anche ore.

La verifica ed eventuale modifica della difficoltà avviene ogni 2016 blocchi, e poiché mediamente viene minato un blocco ogni 10 minuti, questa regolazione avviene circa ogni 2 settimane.

La difficoltà è il numero approssimativo di hash necessari per estrarre un singolo blocco.

Una sequenza di blocchi con la stessa difficoltà viene indicata come Difficulty Epoch.

Al 2.016° blocco della difficulty epoch, la difficoltà viene quindi ricalcolata. Se i blocchi sono stati minati in media più velocemente di 10 minuti, la difficoltà aumenta ovvero il target hash diminuisce. Se i blocchi vengono estratti più lentamente, la difficoltà diminuisce ovvero il target aumenta.

La semplice formula per calcolare il livello di difficoltà è la seguente:

```
Difficulty = Difficulty Target / Target attuale
```

Il Difficulty Target è l'obiettivo più alto possibile da raggiungere con l'hash di un blocco.

Target attuale è la difficoltà derivata dal numero di 256 bit nel Block header.

A questa formula vanno aggiunti dei limiti: la difficoltà non può essere modificata al di sopra o al di sotto di quattro volte il livello di difficoltà corrente. Il limite superiore per ogni difficulty epoch è una modifica del +300%, mentre quello inferiore è una modifica del -75%. Questa regola è stata introdotta per eliminare bruschi cambiamenti della difficoltà.

Se da un lato la Difficulty Adjustment garantisce la prevedibilità dell'offerta di Bitcoin, dall'altro è un:

- meccanismo di sicurezza fondamentale
- meccanismo di autoregolazione
- componente cruciale del consenso

In genere è un buon segno quando il mining di bitcoin diventa più difficile perché significa che è necessaria più potenza da parte dei miner, rendendo più difficile per un attaccante impegnare potenza di calcolo per produrre blocchi manomessi, migliorando la sicurezza della rete.

Nonostante l'aggiustamento della difficulty sia stata teorizzata in modo che si basi sui 2016 blocchi precedenti, in realtà un errore nel protocollo originale di

Bitcoin fa sì che gli aggiustamenti del livello di difficoltà si basino sui 2015 blocchi precedenti.

L'algoritmo del Difficulty Adjustment è vulnerabile all'attacco di tipo timewarp, che è estremamente difficile da effettuare nella mainnet, mentre è più facile nella testnet.

Difficulty bomb

Livello: intermedio

Argomento: tecnologia

La difficulty bomb, è una specie di pillola avvelenata inserita all'interno del codice di Ethereum che costringe ad effettuare continui aggiornamenti al codice e al protocollo Ethereum, introdotto in particolare per garantire che si sia costretti agli aggiornamenti in vista del passaggio ad Ethereum 2.0 che dovrebbe sostituire il meccanismo di consenso da POW a PoS. Come indica il nome, la difficulty bomb è un meccanismo che se non viene disinnescato da un cambiamento aumenterà la difficoltà di verifica del blocco, con una velocità progressiva tale da rendere ad un certo punto impossibile estrarre un nuovo blocco a causa della proibitiva difficoltà.

Difficulty epoch

Livello: intermedio

Argomento: tecnologia

La difficoltà, o Difficulty, del mining Bitcoin viene regolata automaticamente ogni 2016 blocchi in un processo noto come Difficulty Adjustment o "aggiustamento della difficoltà".

Il periodo di tempo di 2016 blocchi nei quali la difficoltà è la stessa viene chiamato Difficulty Epoch.

Poiché mediamente viene minato un blocco ogni 10 minuti, questa regolazione ogni 2016 blocchi avviene circa ogni 2 settimane.

Digest

Livello: avanzato

Argomento: tecnologia

Il digest delle transazioni Bitcoin è un valore hash univoco che rappresenta l'intera transazione e viene utilizzato per creare e verificare le firme digitali necessarie per validare le transazioni sulla rete Bitcoin.

In altre parole, quando una transazione viene creata, viene calcolato un hash della transazione intera utilizzando l'algoritmo di hashing SHA-256. Questo hash è chiamato "digest della transazione".

Una volta che il digest della transazione è stato calcolato, viene utilizzato per creare una firma digitale con la chiave privata del mittente. La firma viene poi inclusa nella transazione e utilizzata per verificare che il mittente abbia autorizzato la transazione.

Quando la transazione viene trasmessa sulla rete Bitcoin, gli altri nodi della rete verificano la firma digitale utilizzando il digest della transazione e la chiave pubblica del mittente. Se la firma è valida, la transazione viene accettata e inclusa nel registro distribuito delle transazioni Bitcoin, chiamato blockchain.

In sintesi, il digest della transazione è un hash della transazione che viene utilizzato per creare e verificare le firme digitali e garantire l'autenticità e l'integrità delle transazioni sulla rete Bitcoin.

DigiCash

Livello: avanzato

Argomento: economia

DigiCash era una forma di valuta digitale creata da David Chaum nel 1989 e dichiarò bancarotta nel 1998.

DigiCash sviluppò eCash, un sistema ideato sempre da David Chaum che permetteva di effettuare transazioni digitali anonime attraverso una tecnologia chiamata blind signature (firma cieca). Questo metodo consentiva alle banche di emettere moneta digitale e trasferirlo in modo anonimo senza poter tracciare le transazioni individuali degli utenti, permettendo agli utenti di conservare denaro come dati sui loro computer.

L'utente doveva scaricare e installare il software di eCash e successivamente aprire un conto corrente in una delle banche aderenti al circuito.

Dopo l'apertura del conto l'utente doveva depositare denaro contante e in cambio la banca emetteva e inviava l'equivalente in moneta elettronica sul computer del cliente. La moneta era spendibile in tutti i negozi che accettavano eCash.

In pratica le banche emettevano moneta elettronica anonima che gli utenti potevano utilizzare per effettuare transazioni senza rivelare la propria identità.

Tuttavia, DigiCash ebbe difficoltà a diffondersi su larga scala a causa della necessità di collaborazione con le banche tradizionali e richiedeva un'entità centrale per sincronizzare le transazioni, poiché il sistema non era decentralizzato come lo è Bitcoin. L'azienda dichiarò bancarotta nel 1998.

Le lezioni apprese da DigiCash sono state importanti per le scelte effettuate per l'implementazione di Bitcoin.

Mentre DigiCash riusciva a risolvere il problema della doppia spesa con un operatore centrale, Bitcoin ha introdotto una soluzione innovativa a questo problema senza la necessità di un punto centrale di fallimento, utilizzando un sistema di consenso decentralizzato che elimina la necessità di un operatore centrale.

Anonimato vs Pseudonimato: eCash di DigiCash garantiva un anonimato quasi totale grazie alle blind signature, mentre Bitcoin offre solo pseudonimato, poiché tutte le transazioni sono registrate pubblicamente sulla blockchain, anche se gli indirizzi non rivelano direttamente l'identità degli utenti.

Meccanismo di consenso: Bitcoin utilizza il Proof of Work per validare le transazioni e prevenire la doppia spesa, mentre DigiCash si affidava a un'entità centrale per evitare problemi di frode.

Digital asset

Bene digitale

Livello: intermedio

Argomento: finanza

Un Digital Asset, asset digitale o più raramente tradotto come un bene digitale, è un termine utilizzato in certi casi come sinonimo di cripto o criptovaluta, di token.

Sebbene questi termini siano spesso usati in modo intercambiabile, si differenziano per una serie di aspetti fondamentali. In generale, un bene digitale è un bene non tangibile che viene creato, scambiato e conservato in formato digitale. Nel contesto della blockchain, gli asset digitali includono criptovalute e token crittografici, e in questi casi è bene digitale scarso, trasferibile elettronicamente e immateriale con un valore di mercato. Le criptovalute e i token sono sottoclassi uniche di asset digitali che utilizzano la crittografia, una tecnica di cifratura avanzata che assicura l'autenticità degli asset crittografici eliminando la possibilità di contraffazione o di doppia spesa.

La differenza fondamentale tra le due classi di asset digitali è che le criptovalute sono l'asset nativo di una blockchain - come BTC o ETH - mentre i token sono creati come parte di una piattaforma costruita su una blockchain esistente, come i numerosi token ERC-20 che costituiscono l'ecosistema Ethereum.

In altri casi digital asset è una risorsa digitale che può essere utilizzata per generare valore. Può essere un file, un'immagine, un video o qualsiasi altra cosa che sia in formato digitale.

Digital signature

Firma digitale

Livello: base

Argomento: tecnologia

Un codice generato mediante crittografia a chiave pubblica e allegato a un documento o un messaggio al fine di verificarne il contenuto.

DINO

Acronimo di: Decentralized In Name Only

Decentralizzato solo di nome

Livello: intermedio

Argomento: politica

È un acronimo per definire le altcoin, che nonostante facciano grandi discorsi sulla decentralizzazione, sono decentralizzate solo di nome e sono completamente centralizzate in tutto ciò che conta. Ciò significa che ci sono rischi significativi sia interni (furto, inflazione, censura) che esterni (regolamenti, acquisizioni forzate, tasse). In altre parole, si tratta di progetti fragili e la dipendenza da essi è un rischio enorme.

Dip

Livello: intermedio

Argomento: finanza

usato nell'espressione "buy the dip" viene inteso come l'acquisto a prezzi di saldo a seguito di forti crolli

distributed

distribuito

Livello: base

Argomento: tecnologia

Un sistema distribuito si riferisce alla suddivisione delle risorse, dei dati o delle funzionalità su più nodi o dispositivi fisici interconnessi. In un sistema distribuito, le diverse componenti lavorano in parallelo per raggiungere un obiettivo comune. Ogni nodo o dispositivo contribuisce alle operazioni e può scambiare informazioni o risorse con gli altri nodi. L'obiettivo principale di un sistema distribuito è la collaborazione e la condivisione delle risorse tra i nodi per migliorare l'efficienza, la scalabilità e la ridondanza del sistema. Un esempio comune di sistema distribuito è Internet, in cui i dati sono suddivisi e trasmessi attraverso una vasta rete di server e dispositivi interconnessi.

Spesso quando si confrontano sistemi o reti in relazione alla loro centralizzazione, viene fatto riferimento ai modelli descritti da Paul Baran che li distingue in:

- centralizzati,
- decentralizzati,
- e distributi.

La differenza tra "decentralizzato" e "distribuito" riguarda principalmente la struttura e l'organizzazione di un sistema o di una rete.
Distribuito può indicare che il calcolo è distribuito su più nodi anziché su uno solo, decentralizzato che nessun nodo sta impartendo istruzioni ad altri nodi su cosa fare.

Poiché il ledger di Bitcoin, il libro mastro, non si trova più in un unico luogo, lo chiamiamo distribuito e, poiché non c'è una parte centrale che se ne occupa, lo chiamiamo decentralizzato. In questo modo si risolve il problema dell'eliminazione dell'intermediario.

In sintesi, la decentralizzazione si riferisce alla distribuzione del potere decisionale e del controllo, mentre la distribuzione si riferisce alla suddivisione delle risorse o delle funzionalità su più nodi o dispositivi. Tuttavia, è importante notare che i concetti di decentralizzazione e distribuzione possono essere interconnessi e spesso coesistono in vari sistemi e reti complessi.

Bitcoin è sia distribuito che decentralizzato. La rete di Bitcoin è distribuita perché le transazioni e i dati associati sono archiviati su molti nodi nella rete, chiamati full node (nodi completi). Ogni full node ha una copia dell'intera blockchain di Bitcoin e partecipa al processo di convalida e propagazione delle transazioni.

Allo stesso tempo, Bitcoin è anche decentralizzato perché non esiste un'autorità centrale che controlli o gestisca la rete. Le decisioni riguardanti il funzionamento del protocollo e la validazione delle transazioni sono prese da un consenso tra i partecipanti alla rete. Non c'è un singolo nodo o entità che possa impartire istruzioni agli altri nodi o prendere decisioni unilaterali.

La combinazione di distribuzione e decentralizzazione fa sì che Bitcoin sia resiliente, sicuro e resistente alla censura. Ogni nodo completo ha una copia indipendente della blockchain e partecipa alla verifica delle transazioni, garantendo che la rete continui a funzionare anche in presenza di guasti o attacchi mirati a un singolo nodo o gruppo di nodi.

Distributed Ledger

Livello: base

Argomento: tecnologia

È un Ledger che non ha un'amministrazione centralizzata e in cui nessuna voce è sotto controllo. I suoi dati digitali sono replicati, condivisi e sincronizzati distribuiti geograficamente su più siti, paesi o istituzioni. Vedi DLT

DLC

Acronimo di: Discreet Log Contract

Contratti a Registro Discreto

Livello: avanzato

Argomento: tecnologia

I DLC, Discreet Log Contracts o Contratti a Registro Discreto, sono smart contract basati su Bitcoin in cui due o più parti bloccano fondi in un indirizzo multisig, e l'oracolo pubblica le informazioni specificate in un momento specifico, come il risultato di una partita sportiva o la quotazione di un prezzo di un asset da parte di un exchange.
L'oracolo non ha bisogno di conoscere i termini del contratto. Il protocollo DLC rende le transazioni indistinguibili da molte altre transazioni Bitcoin e può essere eseguito all'interno di un canale Lightning Network.
Inoltre, i DLC sono argomentabilmente più sicuri dei precedenti metodi basati su oracoli perché un oracolo che si impegna in un falso risultato genera chiare prove di frode.

La parola *discreet* è stata scelta come gioco di parole partendo dal discrete log problem, il problema del logaritmo discreto che è un problema matematico fondamentale nell'ambito della crittografia e della teoria dei numeri, storpiando la parola discrete in discreet che si riferisce più all'aspetto della privacy.

Il fatto che le transazioni che creano e regolano il contratto possano essere rese indistinguibili da altre transazioni Bitcoin o possono essere eseguite all'interno di un canale Lightning rende i DLC più privati ed efficienti rispetto ad altri metodi di contratto basati su oracoli.
I DLC offrono un miglioramento rispetto ad altri tipi di smart contract in quanto il loro impatto sulla blockchain non è diverso da quello di una transazione multisig normale. Tuttavia, i DLC non risolvono completamente il problema degli oracoli, l'incapacità di incorporare dati del mondo reale in un contratto intelligente in modo affidabile.

Con i DLC due o più parti concordano di scambiare denaro a seconda dell'esito di un certo evento determinato da un oracolo (o da diversi oracoli). Per costruire un DLC, due parti bloccano fondi in un indirizzo multisig. Questi fondi possono essere spesi solo quando l'oracolo rilascia le informazioni specificate in un momento specifico. Dopo che l'evento si è verificato, l'oracolo pubblica un commitment o impegno sull'esito dell'evento che la parte vincente può utilizzare per reclamare i propri fondi. L'oracolo non ha bisogno di conoscere i termini del contratto (o persino che un contratto sia stato stipulato). Un oracolo per un DLC può essere qualsiasi tipo di feed di dati, come la pubblicazione da parte di un sito web del risultato di una partita sportiva o la quotazione di un prezzo di un asset da parte di un exchange.
Tuttavia, i DLC non risolvono completamente il problema degli oracoli,

l'incapacità di incorporare dati del mondo reale in un contratto intelligente in modo affidabile, poiché si basano ancora su un oracolo affidabile per rilasciare dati veri.

La costruzione originale dei DLC era specifica per le firme Schnorr. Successivamente è stata sviluppata una versione per utilizzare adattatori di firma che sono compatibili con il sistema di firma ECDSA già esistente di Bitcoin prima dell'introduzione delle firme Schnorr.

Un DLC funziona utilizzando la firma dell'oracolo di un determinato messaggio come chiave privata, il che consente al vincitore della scommessa di firmare una transazione che spende i fondi che le due controparti hanno impegnato all'inizio del contratto.

Ad esempio, se Alice e Bob desiderano creare un DLC per scommettere sull'esito di un lancio di moneta, creano innanzitutto una transazione di finanziamento, in cui entrambe le parti inviano bitcoin, ad esempio 1 BTC ciascuno, a un multisig 2-su-2. Successivamente, Alice e Bob ottengono chiavi pubbliche le cui chiavi private sono appena state create dalla firma dell'oracolo di entrambi gli eventi - testa o croce nel caso di un lancio di moneta. Si noti che queste chiavi private non sono la chiave privata utilizzata per creare le firme degli eventi. Una firma non può essere utilizzata per derivare la chiave privata che l'ha creata.

Con queste chiavi pubbliche, Alice e Bob creano due transazioni di commitment o impegno, chiamate CET, Contract Execution Transactions o Contratti di Esecuzione, una delle quali spende i 2 BTC della transazione di finanziamento alla chiave pubblica *testa* e l'altra alla chiave pubblica *coda*. Entrambe queste transazioni richiedono firme da parte di Alice, Bob e la chiave pubblica *testa* o *coda*. Poiché né Alice né Bob hanno la chiave privata *testa* o *coda*, queste transazioni hanno solo 2 delle 3 firme richieste e rimangono non pubblicate sulla blockchain per il momento.

Dopo che l'oracolo determina il risultato del lancio della moneta, ad esempio *testa*, l'oracolo pubblica la firma corrispondente a *testa* e Alice o Bob utilizzano questa firma per derivare la chiave privata *testa*. Alice e Bob possono ora firmare solo il CET che invia i bitcoin alla persona che ha scelto *testa*. Il CET firmato viene pubblicato sulla blockchain e il vincitore della scommessa riceve i 2 BTC. Il CET che richiedeva la firma *coda* è obsoleto e viene scartato.

Per incentivare il perdente della scommessa a firmare e pubblicare la transazione, viene aggiunto bitcoin extra alla transazione di finanziamento da entrambe le controparti. Se la scommessa è di 1 BTC, ogni controparte potrebbe scommettere 1,5 BTC. Il vincitore riceverà quindi 2,5 BTC e il perdente avrà restituiti i suoi 0,5 BTC. Ciò consente di implementare una condizione di time lock, secondo la quale, se il perdente non ha firmato e pubblicato la transazione entro un certo tempo, il vincitore potrebbe inoltre reclamare i 0,5 BTC di garanzia del perdente.

DLT

Acronimo di: Distributed Ledger Technology

Tecnologia a registro distribuito

Livello: base

Argomento: tecnologia

Un registro distribuito è un insieme di dati digitali replicati, condivisi e sincronizzati, geograficamente distribuiti su più siti, paesi o istituzioni sulla base di un meccanismo di consenso . A differenza di un database centralizzato, non esiste un amministratore centrale.

Don't Trust, Verify

Non fidarti, verifica

Livello: base

Argomento: politica

Il detto "Don't Trust, Verify", in italiano "non fidarti, verifica" significa che non bisogna fidarsi ciecamente di nessuno, ma è necessario verificare le informazioni prima di prendere qualsiasi decisione.

Nel caso di Bitcoin, non solo si invita ad effettuare le verifiche invece di fidarsi, ma anche che non c'è la necessità di avere dei soggetti nei quali porre la propria fiducia, perché basta verificare in quanto le regole del protocollo consentono di avere alla base della validità delle transazioni le regole matematiche e crittografiche.

Un idioma utilizzato per evidenziare la caratteristica dei bitcoin che non si basa sulla fiducia in soggetti definiti appunto fiduciari, ma sul protocollo che consente a chiunque di effettuare le verifiche in modo indipendente.

Nel caso di Bitcoin questo è possibile anche perché:

- Il codice sorgente di Bitcoin è open source, il che significa che chiunque può accedervi e verificarlo. È importante verificare il codice sorgente per assicurarsi che non contenga vulnerabilità di sicurezza o codice dannoso.

- La block chain di Bitcoin è un registro pubblico di tutte le transazioni Bitcoin. È possibile verificare la block chain per assicurarsi che sia accurata e non sia stata manomessa, e che le transazioni siano realmente avvenute.
- Il protocollo Bitcoin è pubblico

DOS

Acronimo di: Denial of Service

Livello: intermedio

Argomento: tecnologia

Un attacco denial-of-service o attacco DoS (lett. "attacco di negazione del servizio") indica un malfunzionamento dovuto a un attacco informatico in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio, fino a renderlo non più in grado di erogare il servizio ai client richiedenti.

Il denial of service si realizza tipicamente inondando la macchina o la risorsa bersaglio di richieste superflue nel tentativo di sovraccaricare i sistemi e impedire che alcune o tutte le richieste legittime vengano soddisfatte.

Double Spend

Doppia spesa

Livello: base

Argomento: tecnologia

Un double spend si verifica quando qualcuno è in grado di spendere due volte gli stessi soldi, ingannando una o più parti facendole credere di essere state pagate.

Gli oggetti digitali come file e testo sono facili da duplicare. Tuttavia, la duplicazione non è una caratteristica desiderabile per il denaro. Questo è il problema della doppia spesa: come può un destinatario di denaro digitale essere sicuro che il denaro che gli è stato inviato non sia stato inviato contemporaneamente a qualcun altro? Come possono tutti i membri di un network monetario essere sicuri che gli altri non duplicano i loro soldi a piacimento?

Bitcoin risolve il problema della doppia spesa utilizzando un registro decentralizzato a cui tutti gli utenti possono accedere. Quando un utente invia bitcoin a un altro, distruggono la moneta che possiede e creano una nuova moneta di proprietà del destinatario. La distruzione della moneta del mittente viene registrata in modo che tutti possano vederla, in modo che non possano mai inviarla a qualcun altro.

Il double spend può verificarsi in alcune criptovalute quando vengono compromesse da malintenzionati, a volte inviando più pacchetti relativi a una transazione alla rete della valuta, ma poi annullano tali transazioni con l'intenzione di far sembrare che non siano mai avvenute.

Un double spend può essere il risultato di un race attack o di un attacco del 51%. Il mining di Bitcoin e della blockchain sono progettati per evitare che questo tipo di attacco possa essere portato a buon fine.

Un double spend tramite race attack è avvenuto ad un operatore di ATM Bitcoin in Canada nel settembre 2018. Quattro persone (molto probabilmente operanti come gruppo coordinato) hanno condotto 112 transazioni presso gli

sportelli ATM di bitcoin e hanno ottenuto 195000 dollari canadesi in contanti. L'attacco è stato condotto in 7 città ed è durato 10 giorni: inviavano bitcoin o altre criptovalute all'ATM e ricevevano contanti. Se l'ATM supporta operazioni di prelievo a fronte di una transazione 0-conf, introduce il rischio di una double spend: dopo aver prelevato contanti dall'ATM, l'attaccante invia un'altra transazione alla rete con fee più elevate e inoltra i fondi al proprio indirizzo bitcoin. Se i miner sostituiscono la transazione iniziale con una nuova e la inseriscono nel blocco (e questo è un comportamento generalmente accettato dalla rete), l'attaccante ottiene effettivamente indietro i fondi di criptovaluta e riceve anche contanti dal bancomat.

drivechain

Livello: avanzato

Argomento: tecnologia

Introdotto per la prima volta nel 2015, il concento di Drivechain presenta un modo per scalare Bitcoin utilizzando le sidechain.
Di solito le sidechain hanno delle loro coin o token specifici e derivano la loro sicurezza dalla blockchain con la quale vengono eseguite in parallelo.
Le drivechain, invece, sono sidechain speciali che non hanno una risorsa nativa ma la prendono in prestito dalla catena madre. In questo modo, le Drivechain consentono agli utenti Bitcoin di bloccare BTC in queste drivechain utilizzando un vincolo bidirezionale (two-way peg), che utilizza una prova crittografica per coniare altcoin con le proprie caratteristiche uniche.

Tale funzionalità non è ancora disponibile su bitcoin, ma richiede un soft fork.

Le Drivechain, definite nei BIP300 and BIP301, è una proposta di softfork Bitcoin che permette a Bitcoin di creare, eliminare, inviare BTC a e ricevere BTC da sidechain o Layer-2.
Queste proposte attiverebbero peg trustless peer-to-peer tra Bitcoin e fino a 256 sidechain.

Le sidechain sono blockchain separate collegate alla blockchain principale, mentre le drivechain sono un tipo specifico di sidechain progettate per migliorare l'efficienza e l'evoluzione della blockchain principale attraverso il **merge-mining**. Entrambi i concetti consentono di sperimentare nuove funzionalità senza compromettere la sicurezza della blockchain principale.

BIP 301 Blind Merged Mining Il BIP 301 introduce un nuovo meccanismo di mining chiamato Blind Merged Mining (BMM). Il BMM consente ai miner Bitcoin di effettuare il mining di una sidechain o altcoin senza dover eseguire il software della sidechain, ovvero senza vederlo e quindi in modalità blind. Invece, un utente sidechain separato gestisce il proprio nodo e costruisce il blocco, pagandosi le commissioni di transazione. Quindi utilizza una quantità equivalente di denaro per "acquistare" il diritto di trovare questo blocco, dai miner

convenzionali del layer 1.

Le sidechain Le sidechain create tramite drivechain sono Altcoin che non hanno una moneta nativa: invece, le monete preesistenti da una diversa blockchain devono essere inviate inizialmente.
Queste sidechain potrebbero essere costruite con qualsiasi funzionalità alternativa desiderata dagli sviluppatori, ereditando sia la sicurezza di Bitcoin che la valuta nativa.

Una volta su una sidechain, le monete possono cambiare di mano un numero illimitato di volte e in un numero illimitato di modi nuovi. Di conseguenza, i possessori di BTC possono scegliere di aderire a nuove funzionalità. Nel frattempo, i detentori di Bitcoin che non aderiscono non devono mai preoccuparsi di cosa stia facendo qualsiasi sidechain.

I trasferimenti dalla sidechain alla mainchain (cioè dal Layer 2 al Layer 1) non vengono effettuati tramite verifiable proof (prova verificabile), ma piuttosto tramite **conjecture-and-refutation** (congettura e confutazione).

Dual funding

Livello: avanzato

Argomento: tecnologia

Su Lightning Network, i canali sono aperti e finanziati attraverso la transazione chiamata Funding Transaction. Questa transazione nella implementazione iniziale veniva creata e finanziata solo dal nodo che avviava il canale.

È stata in seguito introdotto il **Dual Funding**, o **Collaborative fund**, una tecnica utilizzata per aprire un canale che coinvolge due parti che contribuiscono entrambe con una quantità di fondi nella creazione del canale.

In un DFC, **Dual Funded Channel**, entrambe le parti hanno la possibilità di inviare e ricevere fondi immediatamente una volta aperto il canale.

Prima dei dual funded channels, il modo in cui gli utenti LN si connettevano alla rete era aprire un canale privato e finanziarlo direttamente. Il problema di questo approccio è che a volte porta a canali sbilanciati. I canali sbilanciati si verificano quando solo un lato del canale dispone di fondi. Sono un problema per gli utenti perché possono tradursi in ritardi nei pagamenti, in quanto l'altra parte deve spostare fondi prima di poter inviare un pagamento.

Il dual funding è utile perché permette a entrambe le parti di avere una maggiore flessibilità nell'utilizzo del canale e di ridurre il rischio di perdere i fondi investiti nel canale.

Possiamo indicare tre vantaggi principali dei DFC:

- È possibile creare un canale con una capacità doppia rispetto ai fondi disponibili. Ad esempio, se avete a disposizione 1 milione di SAT, potete aprire un canale da 2 milioni.
- Il canale appena aperto è immediatamente bilanciato. Quindi, seguendo l'esempio precedente, potrete inviare 1M e ricevere 1M sul vostro nuovo canale da 2M.
- Si dividono i costi di apertura del canale.

Tuttavia, il dual funding richiede una maggiore cooperazione e coordinazione tra le due parti per gestire il canale in modo efficace, non tutti i software gestiscono l'apertura di un canale Dual Funded, e in alcuni casi sono necessari dei tool aggiuntivi.

Il Dual funding consiste nella creazione di un canale di pagamento per LN in cui entrambe le parti possono contribuire con fondi. Il protocollo sottostante, chiamato protocollo di creazione del canale versione 2, può essere utilizzato anche per l'apertura negoziata di single funded channels, ma il suo scopo motivante è quello di fornire supporto al Dual funding.

Le prime analisi di LN hanno stabilito che sarebbe stato molto più semplice costruire un software in cui l'utente che richiede l'apertura di un canale di pagamento contribuisse con tutti i fondi a quel canale e pagasse tutte le sue commissioni onchain, chiamati single funded channels. In questo modo si evitava che gli aggressori potessero aprire liberamente o a basso costo nuovi canali, bloccare i fondi della controparte e poi far pagare alle vittime le commissioni onchain per riavere i loro soldi.

Per gli spender, i single funded channels funzionano benissimo. Non appena un canale viene aperto, l'utente può iniziare a spendere i propri fondi con tutti i vantaggi di velocità, efficienza e privacy offerti da LN. Ma i receiver che aprono un nuovo canale a finanziamento singolo non possono utilizzarlo per ricevere fondi finché non li hanno spesi. Questo crea problemi ai merchant che vogliono accettare pagamenti su LN, ma che non sono ancora in grado di pagare una quantità uguale di costi su LN.

Una soluzione a questo problema è quella di permettere ai canali di avere un Dual funding, consentendo immediatamente di spendere in entrambe le direzioni una volta aperto il canale. Non è necessario che i canali a Dual funding inizino con la stessa quantità di fondi da entrambe le parti, quindi un commerciante che vuole essere in grado di ricevere una quantità significativa di bitcoin può avere bisogno di contribuire solo a una piccola parte della capacità totale del canale.

Il protocollo a Dual funding può essere utilizzato anche per aprire nuovi single funded channels. Questo può avere dei vantaggi quando le parti partecipanti vogliono utilizzare la capacità del protocollo di comunicare le preferenze dei nodi e trovare valori reciprocamente accettabili per i vari parametri del canale.

Il Dual funding può essere utilizzato in combinazione con le nuove proposte di

annuncio dei nodi che possono aiutare gli acquirenti e i venditori di capacità inbound a trovarsi reciprocamente in modo decentralizzato.

Il Dual funding richiede che ogni parte riveli la proprietà di uno dei propri UTXO all'altra parte. Come altri protocolli in cui ciò è richiesto (come coinjoin e payjoin), questo può essere abusato da un aggressore per ottenere informazioni su chi possiede quale UTXO. Sono stati discussi diversi approcci per limitare questo problema.

dust

Livello: intermedio

Argomento: politica

Un UTXO il cui importo è così piccolo che le commissioni o fee per spenderlo possono essere superiori al suo valore, viene chiamato Dust (povere in italiano).

Con l'aumento delle commissioni, una quantità sempre maggiore di bitcoin possono diventare dust.

Per evitare che gli utenti creino output antieconomici che aumentino le dimensioni dell'UTXO Set, Bitcoin Core e altri nodi si rifiutano di trasmettere o minare transazioni con output inferiori a un certo valore, chiamato dust limit.

Per ridurre il rischio che nel proprio wallet i bitcoin si possano trasformare in dust, può essere una buona norma consolidare le quantità molto piccole di bitcoin in un unico importo più grande in un momento in cui le commissioni sui bitcoin sono basse.

Bitcoin Core imposta il dust limit a un valore in cui la spesa di un output supererebbe 1/3 del suo valore. Questo calcolo si basa sull'impostazione -minrelaytxfee del nodo, il minimum relay transaction fee: per un nodo che utilizza il valore predefinito -minrelaytxfee di 0,00001 BTC/KB (1000 satoshis/KB) e dato che per P2PKH un input è di 148 byte e un output è di 34 byte, ne consegue che un output inferiore o uguale a **546** satoshi è considerato dust da Bicoin core.

A volte il termine Dust viene usato come sinonimo di output antieconomico o, più genericamente, di output di basso valore. Questo può creare confusione, come nel caso di dust attack che coinvolgono quantità appena superiori al limite del dust.

È possibile creare "dust collector" attraverso l'impostazione del Sighash flag con il valore SIGHASH_NONE|ANYONECANPAY: con questo tipo di firma, le UTXO dust possono essere donati perché chiunque possa aggregarli e spenderli quando vuole.

dust attack

Livello: intermedio

Argomento: tecnologia

Il Dust Attack è un tipo di attacco effettuato tramite transazioni di piccoli importi chiamate dust.

In un dust attack, un attaccante invia piccole quantità di bitcoin a indirizzi che sono già apparsi sulla blockchain, producendo un riutilizzo degli indirizzi anche per gli utenti che consapevolmente hanno cercato di evitarlo.

dutch auction

asta olandese o asta al ribasso

Livello: base

Argomento: finanza

Una Dutch auction, asta olandese, asta al ribasso o asta inversa, è uno dei numerosi tipi di aste per l'acquisto o la vendita di merci. Un'asta olandese è un tipo di asta in cui il prezzo inizia alto e diminuisce fino a quando qualcuno non è disposto a pagare per l'oggetto in vendita. A differenza di un'asta tradizionale, in cui i partecipanti fanno offerte sempre più alte fino a quando non viene superato il prezzo di riserva, in un'asta olandese il prezzo diminuisce fino a quando un partecipante è disposto a pagare.

Le aste olandesi sono utilizzate in una varietà di settori, tra cui la pubblicità digitale, i beni immobili e le criptovalute. Le aste olandesi sono particolarmente adatte per la vendita di beni che hanno un valore volatile, come le criptovalute. Questo perché le aste olandesi consentono ai venditori di fissare un prezzo minimo per il loro bene, ma allo stesso tempo di garantire che il bene venga venduto al prezzo più alto possibile.

Le aste olandesi possono essere implementate in diversi modi, ma il metodo più comune è utilizzare un sistema di offerte a ribasso. In un sistema di offerte a ribasso, il venditore stabilisce un prezzo iniziale per il suo bene e quindi inizia a ridurre il prezzo in modo incrementale. I compratori possono quindi fare offerte per il bene al prezzo corrente. L'offerta più alta vince l'asta e il compratore deve pagare il prezzo corrente del bene.

Le aste olandesi sono un metodo efficiente e trasparente per vendere beni. Sono inoltre sicure per i compratori, in quanto i compratori sanno sempre il prezzo massimo che dovranno pagare per il bene.

Aste olandesi con PSBT

I PSBT (Transazioni Bitcoin Parzialmente Firmate) sono un tipo di transazione Bitcoin che non è ancora stata firmata da tutti i partecipanti. I PSBT possono

essere utilizzati per implementare aste olandesi Bitcoin in modo decentralizzato.

In un'asta olandese Bitcoin, il venditore crea un PSBT con un prezzo iniziale alto. Il venditore quindi invia il PSBT ai potenziali compratori. Se nessuno fa un'offerta per il bene, il venditore può abbassare il prezzo del PSBT e inviarlo nuovamente ai potenziali compratori. Il processo continua fino a quando qualcuno fa un'offerta per il bene.

Una volta che qualcuno fa un'offerta per il bene, il venditore deve firmare il PSBT. Il compratore quindi deve firmare il PSBT e inviarlo al venditore. Una volta che il venditore ha ricevuto il PSBT firmato dal compratore, la transazione viene inviata alla rete Bitcoin per essere confermata.

Le aste olandesi Bitcoin sono un modo efficiente e sicuro per vendere beni utilizzando Bitcoin. Sono inoltre decentralizzate, il che significa che non richiedono la fiducia in un'autorità centrale.

Vantaggi delle aste olandesi Le aste olandesi offrono una serie di vantaggi rispetto ad altri tipi di aste, tra cui:

- **Efficienza**: le aste olandesi possono essere condotte in modo rapido ed efficiente.
- **Trasparenza**: i compratori sanno sempre il prezzo massimo che dovranno pagare per il bene.
- **Sicurezza**: le aste olandesi sono sicure per i compratori, in quanto non richiedono la fiducia in un'autorità centrale.
- **Decentralizzazione**: le aste olandesi sono decentralizzate, il che significa che non richiedono la partecipazione di un'autorità centrale. Applicazioni delle aste olandesi

Le aste olandesi possono essere utilizzate per vendere una varietà di beni, tra cui:

- Criptovalute
- Beni immobili
- Opere d'arte
- Collezionabili
- Beni digitali
- Le aste olandesi sono un metodo versatile e flessibile che può essere utilizzato per vendere una varietà di beni in modo efficiente, sicuro e trasparente.

DYOR

Acronimo di: Do Your Own Research

Fai la tua ricerca

Livello: intermedio

Argomento: legale

DYOR è un acronimo inglese che significa "Fai la tua ricerca indipendente" o "Fai la tua ricerca personale".

Viene spesso utilizzato come avvertimento per gli investitori a non basare le loro decisioni su consigli o informazioni ricevute da fonti non verificate e a condurre la propria ricerca prima di prendere qualsiasi decisione di investimento.

È una formula standard utilizzata per indicare che ognuno deve farsi una propria idea effettuando degli approfondimenti.

Viene a volte usata da chi da consigli che *non sono consigli finanziari*, per evitare responsabilità e spesso senza specificare come e dove debbano essere fatte queste ricerche.

E-gold

Livello: intermedio

Argomento: tecnologia

E-gold era un sistema di moneta digitale fondato nel 1996 da Douglas Jackson e Barry Downey, progettata per consentire pagamenti elettronici garantiti da riserve auree. Permetteva agli utenti di aprire conti denominati in oro e di effettuare transazioni online con altri utenti. Ogni unità di e-gold rappresentava un grammo di oro fisico, custodito in depositi sicuri.
I founder sono stati processati e condannati.

E-gold può essere considerato un precursore di Bitcoin, in quanto condivideva alcune caratteristiche fondamentali:

- **Moneta digitale**: Entrambi operavano come valute digitali, consentendo transazioni online senza intermediari finanziari tradizionali.
- **Decentralizzazione**: E-gold, pur avendo una società di gestione, mirava a operare al di fuori del controllo dei governi e delle banche centrali, similmente a Bitcoin.
- **Riserve**: E-gold era sostenuto da riserve di oro fisico, mentre Bitcoin si basa su un sistema di scarsità digitale e proof-of-work.

Differenze chiave:

- **Tecnologia**: E-gold utilizzava una tecnologia centralizzata, mentre Bitcoin si basa su una blockchain decentralizzata.
- **Anonimato**: E-gold offriva un certo grado di anonimato, ma era comunque soggetto a normative antiriciclaggio. Bitcoin offre un maggiore anonimato, sebbene le transazioni siano registrate sulla blockchain.
- **Scalabilità**: E-gold ha affrontato problemi di scalabilità e sicurezza, che hanno contribuito al suo declino. Bitcoin, sebbene con le sue sfide, ha una maggiore scalabilità grazie a soluzioni come il Lightning Network.

Centralizzazione e vulnerabilità legale: E-gold, pur proponendosi come un sistema decentralizzato, aveva un punto debole fondamentale: era gestito da una singola società, la Gold & Silver Reserve Inc., con sede negli Stati Uniti. Questo ha reso e-gold vulnerabile all'intervento del governo americano, che ha potuto esercitare la sua giurisdizione sull'azienda e sui suoi fondatori. L'accusa di riciclaggio di denaro e l'assenza di licenza per la trasmissione di denaro hanno portato alla chiusura di e-gold.

Bitcoin, al contrario, è veramente decentralizzato. Non esiste un'entità singola o un gruppo di persone che lo controlla. La sua natura distribuita lo rende resistente alla censura e all'intervento governativo. Nessun governo può "spegnere" Bitcoin o confiscare i suoi fondi, come è successo con e-gold.

Dipendenza da un'autorità centrale: E-gold si basava sulla fiducia negli amministratori della Gold & Silver Reserve Inc. per la gestione delle riserve auree e la sicurezza del sistema. Questo ha creato un singolo punto di fallimento. Se l'azienda fosse stata gestita male, attaccata da hacker o soggetta a frodi interne, l'intero sistema sarebbe crollato.

Bitcoin, invece, opera attraverso un consenso distribuito. La validità delle transazioni e la sicurezza del network sono garantite da una rete globale di miners, senza la necessità di un'autorità centrale. Questo rende Bitcoin molto più resiliente agli attacchi e alle frodi.

Confisca delle riserve: Un altro punto debole di e-gold è stata la possibilità per il governo di confiscare le riserve auree dell'azienda. Questo ha dimostrato che, nonostante le promesse di indipendenza da banche e governi, e-gold era comunque vulnerabile all'intervento statale.

Con Bitcoin, questo scenario è impossibile. I bitcoin non sono "custoditi" da nessuno e non possono essere confiscati da un governo. Gli utenti che hanno il controllo completo delle proprie chiavi private hanno anche il controllo dei propri fondi.

In sintesi, e-gold ha precorso i tempi, ma la sua struttura centralizzata lo ha reso vulnerabile a problemi legali e attacchi. Bitcoin, grazie alla sua decentralizzazione e alla tecnologia blockchain, ha superato questi limiti, offrendo un sistema di moneta digitale veramente resistente alla censura e al controllo governativo.

E-gold, pur essendo stato chiuso nel 2009, ha avuto un ruolo importante nello sviluppo delle valute digitali. Ha dimostrato la fattibilità di un sistema di pagamento online basato su riserve e ha anticipato alcune delle caratteristiche chiave di Bitcoin. Tuttavia, la tecnologia blockchain di Bitcoin ha superato i limiti di E-gold, aprendo la strada a un nuovo ecosistema finanziario decentralizzato.

Easy money

Livello: base

Argomento: economia

Easy money, fa riferimento a una forma di denaro che è abbondante, facilmente disponibile e può essere creato con facilità, contrariamente all'Hard money.

Il termine "easy money" si riferisce a una politica monetaria espansiva adottata da alcune banche centrali, in cui si aumenta la quantità di denaro in circolazione per stimolare la crescita economica.

L'obiettivo principale dell'easy money è quello di incentivare la spesa e gli investimenti, incoraggiando così la crescita economica.

Tale politica monetaria espansiva attuataper aumentare la quantità di moneta in circolazione può essere realizzata attraverso una serie di strumentio misure, tra cui:

- Abbassare i tassi di interesse
- Acquistare attività finanziarie, in particolare obbligazioni governative o titoli di stato
- Emettere nuova moneta
- implementazione di programmi di stimolo economico.

Ad esempio le valute tradizionali, o fiat, come il dollaro statunitense o euro sono controllate da banche centrali e governi, che possono creare nuova moneta a loro discrezione attraverso politiche di stampa di denaro o interventi monetari o Quantitative Easing.

Se la quantità di denaro emessa aumenta in modo sproporzionato rispetto alla crescita economica reale, possono verificarsi problemi come l'inflazione, l'instabilità economica e altri rischi finanziari.

Per quanto riguarda i bitcoin, essi non possono essere considerati "easy money" poiché sono una forma di denaro digitale decentralizzato e limitato nella quantità. Il protocollo Bitcoin è progettato per essere deflazionistico, il che significa che nel tempo il tasso di emissione di nuovi bitcoin diminuisce progressivamente e si stabilizzerà intorno a 21 milioni di bitcoin in circolazione.

Il rilascio di nuovi bitcoin avviene tramite un processo chiamato mining, in cui i miner (coloro che partecipano alla rete Bitcoin) devono effettuare impegnativi matematici per confermare le transazioni e creare nuovi blocchi di transazioni. Il numero di nuovi bitcoin creati per blocco viene dimezzato approssimativamente ogni 4 anni in un evento noto come "halving". Questo meccanismo di rilascio controllato impedisce la creazione arbitraria di nuovi bitcoin e limita la loro quantità massima a 21 milioni.

Inoltre, i Bitcoin sono una valuta decentralizzata, il che significa che non sono soggetti al controllo di alcun governo o banca centrale. Questo rende i Bitcoin

meno vulnerabili alle politiche monetarie espansive, che possono portare a un deprezzamento delle valute fiat.

Pertanto, a differenza delle valute fiat, i bitcoin hanno una quantità fissa e limitata, rendendoli un bene deflazionistico e contrastando il concetto di easy money. Non possono essere emessi o prodotti arbitrariamente, e il loro valore è influenzato dalla domanda e dall'offerta sul mercato, oltre ad altri fattori economici e di mercato.

EBA

Acronimo di: European Banking Authority

Autorità bancaria europea

Livello: intermedio

Argomento: politica

L'EBA European Banking Authority, in italiano Autorità bancaria europea, è un organismo dell'Unione europea che dal 1º gennaio 2011 ha il compito di sorvegliare il mercato bancario europeo.

ECash

Livello: avanzato

Argomento: tecnologia

eCash, o Chaumian eCash, si riferisce a un tipo di sistema di denaro elettronico proposto da David Chaum, un crittografo e ricercatore nella sicurezza informatica. La sua idea era di creare un sistema di pagamento elettronico che fornisse un alto grado di privacy e anonimato per gli utenti, simile al contante fisico.

Il concetto chiave dietro il Chaumian eCash è l'utilizzo di firme digitali cieche (blind signatures) e altre tecniche crittografiche per garantire l'anonimato delle transazioni. In una firma digitale cieca, un utente può ottenere una firma valida senza rivelare il contenuto del messaggio a chi fornisce la firma. Questo permette agli utenti di effettuare transazioni senza rivelare le proprie identità o i dettagli delle transazioni stesse.

Il sistema Chaumian eCash avrebbe consentito agli utenti di trasferire denaro in modo anonimo e sicuro su Internet, fornendo una forma di pagamento elettronico simile al contante in termini di anonimato. Tuttavia, nonostante le sue potenzialità, il concetto di Chaumian eCash non è stato ampiamente adottato, in parte a causa di sfide regolamentari e di privacy che hanno impedito la sua implementazione su larga scala.

ECC

Acronimo di: Elliptic-Curve Cryptography

Crittografia a curva ellittica

Livello: avanzato

Argomento: tecnologia

ECC sta per crittografia a curva ellittica. È un ramo specifico della crittografia a chiave pubblica che dipende da calcoli matematici condotti utilizzando curve ellittiche definite su campi finiti. È più complesso e più difficile da spiegare rispetto alla classica crittografia a chiave pubblica (che utilizzava i numeri primi), ma presenta dei bei vantaggi.

Cos'è una curva ellittica?

Una curva ellittica è una curva geometrica che assume la forma $y^2 = x^3 + ax + b$. Una specifica curva ellittica viene scelta selezionando valori specifici di a e b. La curva deve quindi essere esaminata attentamente per determinare se funziona bene per la crittografia. Ad esempio, la curva secp256k1 utilizzata da Bitcoin è definita come a=0 e b=7.

Qualsiasi linea che interseca una curva ellittica lo farà in 1 o 3 punti, e questa è la base della crittografia della curva ellittica.

Come vengono utilizzate le curve ellittiche nella crittografia?

Nella crittografia a curva ellittica, un utente seleziona un numero molto grande (256 bit) come chiave privata. Quindi aggiunge un punto base impostato sulla curva a se stesso molte volte.

È quindi possibile utilizzare varie formule matematiche per dimostrare la proprietà della chiave pubblica, data la chiave privata. Come con qualsiasi funzione crittografica, questa è una trap door, una botola: è facile passare dalla chiave privata alla chiave pubblica e praticamente impossibile passare dalla chiave pubblica alla chiave privata.

Quali sono i vantaggi dell'ECC?

Il principale vantaggio di ECC è che consente la stessa sicurezza della classica crittografia a chiave pubblica con una chiave molto più piccola. Una chiave pubblica a curva ellittica a 256 bit corrisponde a una chiave pubblica tradizionale (RSA) a 3072 bit.

Riassumendo

Un modo per pensare a ECC è: un modo per abilitare la crittografia a chiave pubblica che utilizza chiavi molto piccole e matematica molto oscura.

ECDH

Acronimo di: Elliptic Curve Diffie-Hellman

Curva Ellittica Diffie-Hellman

Livello: avanzato

Argomento: tecnologia

Elliptic-curve Diffie–Hellman (ECDH), Diffie-Hellman a curva ellittica, è un protocollo di scambio sicuro di chiavi che consente a due parti di generare un segreto condiviso su un canale non protetto.

Questo segreto può essere usato direttamente come chiave oppure per derivarne un'altra. La chiave, originale o derivata, viene poi utilizzata per crittografare le comunicazioni successive tramite un cifrario a chiave simmetrica.

Si tratta di una variante del protocollo Diffie-Hellman che sfrutta la crittografia a curva ellittica.

ECDSA

Acronimo di: Elliptic Curve Digital Signature Algorithm

Algoritmo di firma digitale a curva ellittica

Livello: avanzato

Argomento: tecnologia

L'algoritmo di firma digitale a curva ellittica o ECDSA è uno schema crittografico per la produzione di firme digitali utilizzando chiavi pubbliche e private.

Le chiavi e le firme Bitcoin sono attualmente generate per lo più utilizzando ECDSA, alla quale recentemente si sono aggiunte le firme Schnorr.

Una firma ECDSA consente a qualcuno di pubblicare una chiave pubblica e quindi creare una firma di alcuni dati con la propria chiave privata, in modo tale che chiunque possa verificare che la firma sia stata creata dal proprietario di questa chiave pubblica.

Tuttavia, nessuno è in grado di derivare la chiave privata dalla chiave pubblica o dalla firma. Né questa firma può essere utilizzata per falsificare una firma per altri dati.

Le firme ECDSA vengono utilizzate per firmare tutte le transazioni Bitcoin grazie a queste potenti funzionalità di sicurezza.

Una curva ellittica è una funzione matematica definita del formato generale y^2 = x^3 ax b. Per Bitcoin, questa curva ha l'equazione specifica y^2 = x^3 7, come

a = 0 e b = 7. Qualsiasi punto su questa curva ellittica, chiamato secp256k1, è una chiave pubblica Bitcoin valida. Per generare una chiave pubblica, un utente deve generare una chiave privata, che è semplicemente un numero elevato. Successivamente, questa chiave privata viene moltiplicata per un punto definito chiamato Generator Point, per produrre la chiave pubblica. Questa moltiplicazione è una moltiplicazione per punti, che si comporta in modo diverso dalla normale moltiplicazione. Fondamentalmente, la divisione dei punti è incalcolabile, il che significa che una chiave pubblica non può attualmente essere utilizzata per derivare una chiave privata, conferendo allo schema ECDSA la sua sicurezza.

Eclipse attack

Livello: intermedio

Argomento: tecnologia

Gli Eclipse attack si verificano quando un nodo è isolato da tutti i peer onesti ma rimane connesso ad almeno un peer dannoso.

Senza alcuna connessione con peer onesti, il nodo *eclissato* non riceverà gli ultimi blocchi della block chain con maggiore proof-of-work. Questo dà all'attaccante una quantità illimitata di tempo per generare blocchi contenenti doppie spese, quindi anche un attaccante con una piccola minoranza di hash rate può indurre la vittima ad accettare doppie spese confermate.

L'attaccante controllerà anche quali transazioni riceve il nodo della vittima. Ciò consente loro di informare il nodo sulle transazioni non generalmente disponibili sulla rete per indurre il nodo della vittima a intraprendere un'azione (ad esempio, l'attaccante invia una transazione chiudendo un canale Lightning Network solo al nodo eclissato).

Infine, l'aggressore può controllare quali transazioni può inviare la vittima. Ciò consente all'aggressore di impedire alla vittima di inviare transazioni urgenti come le penalty transaction Lightning Network. Significa anche che qualsiasi transazione generata dalla vittima può essere definitivamente identificata come originata dalla vittima: una perdita di privacy.

Per prevenire gli eclipse attacks, gli operatori dei nodi sono incoraggiati a eseguire i propri nodi su più interfacce di rete e, quando possibile, a mantenere connessioni ad almeno alcuni altri nodi su reti sicure (ad es. VPN). Entro i limiti possibili per i nodi con una sola interfaccia, gli sviluppatori di Bitcoin Core lavorano per garantire che il nodo si connetta a un insieme ampio e diversificato di peer per ridurre la possibilità che ognuno dei peer di un nodo sia lo stesso sybil attacker.

Ecofin

Acronimo di: Economic and Financial Affairs Council

Consiglio Economia e finanza

Livello: intermedio

Argomento: politica

Il Consiglio "Economia e finanza" (ECOFIN) è responsabile della politica dell'UE in tre settori principali: politica economica, questioni relative alla fiscalità e regolamentazione dei servizi finanziari.

È una delle formazioni in cui si riunisce il Consiglio dell'Unione europea. E' composto dai ministri dell'economia e delle finanze degli stati membri ed eventualmente dai ministri del bilancio.

Edge liquidity

Livello: avanzato

Argomento: tecnologia

La Edge liquidity descrive il concetto attraverso il quale alcuni nodi Lightning Network, con i quali si hanno canali di asset Taro, possono essere disposti a scambiare il loro valore in BTC e viceversa, consentendo di utilizzare i propri asset Taro per pagare qualsiasi Lightning invoice o ricevere qualsiasi asset emettendo una Lightning invoice standard.

EIP

Acronimo di: Ethereum Improvement Proposal

Proposta di miglioramento di Ethereum

Livello: intermedio

Argomento: tecnologia

Un EIP è un documento di progettazione che fornisce informazioni alla comunità di Ethereum, o che descrive una nuova caratteristica per Ethereum o i suoi processi o ambienti. L'EIP dovrebbe fornire una concisa specifica tecnica della caratteristica e una logica per la caratteristica. L'autore dell'EIP è responsabile della costruzione del consenso all'interno della comunità e della documentazione delle opinioni dissenzienti.

EIP-1559

Livello: avanzato

Argomento: tecnologia

La modifica EIP-1559 è stata introdotta nel protocollo Ethereum con l'hard fork London nell'agosto 2021. Con EIP-1559, ogni transazione su Ethereum

comporta la totale distruzione della “base fee”, riducendo gradualmente l’offerta circolante di Ether (ETH). Con EIP-1559 una transazione è valida solo se la fee massima è maggiore della fee di base più la priority fee. Qualsiasi importo in eccesso viene rimborsato all’utente”,. Di conseguenza, gli utenti avranno molta più certezza quando inviano una transazione perché devono solo assicurarsi di includere abbastanza per pagare la Commissione di base e una piccola commissione di priorità per includere la propria transazione

La EIP-1559 cambierà il meccanismo di determinazione delle commissioni che vengono pagate per ogni transazione su Ethereum. Precedentemente il meccanismo con cui venivano determinate le fee di transazione in Ethereum era il first-price auction: gli utenti facevano un’offerta (con modalità simili a quelle di un’asta) per ottenere dello spazio e includere la propria transazione nel blocco successivo. Questo avveniva definendo il massimo gas price (il gas su Ethereum è proprio la fee pagata dagli utenti per effettuare una transazione) che gli utenti erano disposti a pagare per vedere la propria transazione validata dai miner. Essendo la block size limitata, si genera una competizione per lo spazio al suo interno e gli utenti, che facevano le offerte più alte ai miner che creano i blocchi, vedevano le proprie transazioni scelte per prima. Nei momenti di congestione della rete, questo meccanismo poteva risultare poco efficiente per gli utenti. Nei periodi di congestione accadeva infatti spesso di dover pagare fee molto elevate anche per transazioni semplici. La EIP-1559 cerca migliorare l’esperienza proprio da questo punto di vista, con quattro obiettivi fondamentali: - rendere le fee più facilmente prevedibili; - ridurre il tempo di conferma delle transazioni; - automatizzare il sistema di calcolo delle fee; - creare un circolo virtuoso tra l’attività on-chain e il valore dell’asset ETH. L’obiettivo della EIP-1559 non è, quindi, rendere le transazioni più economiche, ma di rendere le fee più facilmente prevedibili per gli utenti. Per la riduzione delle commissioni sono attualmente in fase di sviluppo altre soluzioni, come i rollup su Layer 2 o il futuro aggiornamento a Ethereum 2.0. La EIP-1559 sostituisce infatti la volatilità delle commissioni con la volatilità della dimensione dei blocchi, rendendo più facile prevedere il costo delle transazioni.

Eltoo

Livello: avanzato

Argomento: tecnologia

Eltoo - pronunciato come si pronuncia in inglese la sigla “L2” (in riferimento a Layer 2) - è una proposta di aggiornamento di Bitcoin il cui obiettivo principale è migliorare le soluzioni di secondo livello, soprattutto la rete Lightning.

Eltoo implementerebbe questi aggiornamenti introducendo nel protocollo Bitcoin un nuovo flag sighash chiamato SIGHASH_NOINPUT, e in seguito SIGHASH_ANYPREVOUT introdotto con il BIP-118. Il nuovo flag sighash consentirebbe a una firma Bitcoin di impegnarsi in una transazione senza specificare il txid dell’input.

Lasciare il txid non specificato consente una maggiore flessibilità per le transazioni. Significa che le transazioni discendenti possono essere firmate prima che i loro antenati siano pubblicati sulla blockchain.

Ad esempio, se Alice e Bob aprono un canale Lightning, prima firmano una funding transaction, che invia bitcoin a un indirizzo multisig 2-di-2. Una volta aperto il canale, Alice e Bob effettuano una serie di transazioni di aggiornamento, che spendono i fondi nell'indirizzo 2-of-2 multisig. Quando Alice e Bob desiderano chiudere il canale, devono firmare una transazione di chiusura del canale, una settlement transaction.

Senza Eltoo, ogni transazione di questo processo può essere firmata solo dopo che la precedente è stata creata. Con Eltoo, la settlement transaction può essere firmata contemporaneamente alla funding transaction. In questo modo si elimina la necessità di una Lightning Network penalty, semplificando notevolmente la protezione contro la double spend sulla rete Lightning.

Poiché Eltoo introdurrebbe un nuovo flag sighash, si tratta di una modifica al protocollo di consenso e richiederebbe un soft fork.

Eltoo è uno schema che realizzerebbe la visione di Satoshi per nSequence consentendo ai peer di scambiare transazioni pre-firmate off-chain incrementando i numeri di sequenza in modo tale che solo l'ultima possa essere pubblicata on-chain.

Con Eltoo si può:

- implementare LN Symmetry, un modo migliore per i canali Lightning, che consente:
  - Watchtower leggere e quasi gratuite
  - Gestione più sicura dei canali senza penalty transaction
  - Possibilità di chiudere completamente un canale da un lato, senza che all'altro lato venga lasciato in uno stato potenzialmente conflittuale
  - Backup del canale molto più semplici
  - Canali multiparty (noti anche come "channel factories")
  - Meno problemi nella stima delle fee che causano sovrapagamenti e chiusure di canali indesiderate
  - Interoperabilità con i canali Lightning esistenti
  - Il protocollo Lot49 per le reti mesh a bassa latenza alimentate da Lightning
  - Complessivamente, un flusso di protocollo molto più semplice che consente un'implementazione più facile di altre idee su Lightning
- Blind Statechains, un protocollo per il trasferimento off-chain di UTXO utilizzando blind server e/o federazioni come terze parti semi-affidabili. Le Statechains possono essere utilizzate:
  - Come meccanismo di trasferimento del valore off-chain in sé, utilizzato per trasferire grandi valori come UTXO singoli e non interrotti (con il cambio fornito con statechains di tagli più piccoli o attraverso altri mezzi)

  - Per aprire i canali Lightning su questi UTXO. E poi questi canali possono essere utilizzati o trasferiti ad altri senza toccare la catena.
  - Per fare tante cose interessanti che coinvolgano la proprietà di UTXO (Ordinals o DLC, per esempio), ma off-chain.

Statechains e persino Lightning su statechains sono già implementati dal wallet Mercury, ma utilizzando un set molto peggiore di trade-off (che sono pronti per essere scambiati per la versione migliorata basata su Eltoo quando questa sarà disponibile)

Emission

Emissione

Livello: base

Argomento: tecnologia

L'Emission, o emissione in italiano, è la velocità con la quale vengono prodotti e rilasciati i nuovi token o coin di una criptovaluta.

Per quanto riguarda Bitcoin, il suo protocollo include un algoritmo che regola la funzione di emissione attraverso il mining. La difficoltà dell'attività di calcolo che i miner devono eseguire viene regolata dinamicamente in modo che in media ogni 10 minuti viene aggiunto un nuovo blocco alla sua block chain.
Al momento del lancio, i miner venivano ricompensati con 50 BTC per ogni blocco convalidato, il che significa che il tasso di emissione di BTC era di circa 7200 Bitcoin al giorno.

Ogni 4 anni circa avviene il dimezzamento dei bitcoin emessi in quel processo chiamato halving, il che significa che il numero di nuovi Bitcoin che entrano nell'ecosistema è diminuito sostanzialmente. A maggio 2020, il numero di Bitcoin in entrata è di 6,25 BTC.

Il risultato è che il numero di bitcoin emessi segue una curva facilmente prevedibile.

Approssimativamente al blocco 1,411,200 che ci si aspetta verrà minato intorno all'anno 2035, il 99% di tutti i bitcoin saranno stati emessi.
L'ultimo BTC in assoluto dovrebbe essere estratto nel 2140 circa, perché ha un'offerta massima di circa 21 milioni.

Alcune criptovalute non hanno un tasso di emissione prestabilito, il che significa che nuove unità possono essere create su richiesta.

Empty block

Blocco vuoto

Livello: intermedio

Argomento: tecnologia

Alcuni blocchi vengono creati senza transazioni dai miner, e aggiunti alla blockchain. Questi blocchi senza transazioni vengono chiamati empty block, blocchi vuoti, ma contengono comuque dati. Non sono privi di dati, semplicemente non contengono transazioni diverse dalla transazione di generazione di monete (nota come transazione coinbase). Poiché un blocco vuoto non contiene alcuna transazione dalla rete Bitcoin, è considerato vuoto.

Anche i blocchi vuoti sono computazionalmente costosi perché i miner devono comunque effettuare i calcoli richiesti dalla Proof of work. Hanno comunque l'intestazione del blocco e hanno tutti i campi dei i blocchi non vuoti. Hanno anche un elenco di transazioni; ma quell'elenco contiene una singola transazione, la transazione coinbase, che paga al miner il Block Reward, il premio per aver minato il blocco anche se vuoto.

I blocchi vuoti non sono del tutto inutili. In primo luogo, estendono la blockchain aggiungendo ulteriore lavoro alla blockchain. Le transazioni all'interno di un blocco non influiscono sulla quantità di lavoro necessaria per minare il blocco, quindi i blocchi vuoti rafforzano la sicurezza della blockchain aggiungendosi al lavoro cumulativo utilizzato per la blockchain. I blocchi vuoti introducono anche nuovi coin nel sistema Bitcoin, pagano comunque i miner per il lavoro che hanno svolto, quindi vengono generate nuove monete e pagate al miner di quel blocco. Questo fa parte della transazione di generazione di monete inclusa nel blocco stesso come unica transazione.

Inoltre, quando non ci sono transazioni nella mempool (evento ormai altamente improbabile), il network deve comunque andare avanti. Devono ancora essere estratti i blocchi, quindi devono essere consentiti blocchi vuoti affinché la blockchain possa continuare.

cosa succede se ci sono esempi di transazioni come l'invio di btc a un altro indirizzo ma nessuno lo estrae (verificandolo tramite mining), le transazioni arriveranno mai all'indirizzo destinato? Se nessuno include mai una transazione in un blocco, la transazione non è mai considerata definitiva. Apparirà ancora nei portafogli degli utenti come non confermato e vedranno le monete. Possono anche spendere gli output di quella transazione, ma non è consigliabile creare transazioni da transazioni non confermate. Anche una tale transazione non sarebbe confermata fintanto che la prima transazione non confermata rimane non confermata.

Ci possono essere diverse motivazioni che portano un miner a non inserire transazioni minando un blocco vuoto, e rinunciando al guadagno aggiuntivo rappresentato dalle fee delle transazioni, la principale è dovuta al fatto che in quel breve intervallo di tempo nel quale che si raccolgono le informazioni su quali transazioni inserire nel blocco, si prova comunque a minare un blocco vuoto, e può accadere che si trovi una soluzione anche in quel breve intervallo di tempo.

I blocchi vuoti erano più frequenti nei primi blocchi della blockchain Bitcoin,

anche perché non c'erano sufficienti transazioni per ogni blocco. Il mining di blocchi vuoti è diventato sempre meno comune nel corso degli anni, e ormai sono sempre più rari i blocchi vuoti inseriti nella blockchain. Sia perché ci sono sempre più transazioni, sia perché non è conveniente per i miner rinunciare alle fee delle transazioni, ma anche perché c'è stata una evoluzione dei sistemi di mining. Tra questi il protocollo Stratum utilizzato dalle mining pool che nella versione V2, diversamente dalla V1 nel quale il trasferimento dei dati che consente ai miner di iniziare a lavorare su un nuovo blocco contiene il modello di blocco con il prevhash insieme, separa questi due componenti. Di conseguenza, le mining pool saranno in grado di scavare più a fondo nella mempool (per le transazioni che è improbabile che vengano incluse nel blocco corrente) e costruire modelli di blocchi completi prima che venga trovato il blocco corrente. Quindi possono inviare quei modelli di blocco ai miner in anticipo quando la latenza non ha importanza, in modo che solo il messaggio prevhash debba essere inviato per iniziare effettivamente il nuovo round di mining.

EMTs

Acronimo di: e-money token

Livello: avanzato

Argomento: politica

EMT o 'electronic money tokens' o 'e-money tokens', è il modo nel regolamento europeo MiCA di chiamare le stablecoin.

Il regolamento le definisce come *"cripto-asset che mirano a stabilizzare il proprio valore facendo riferimento una sola official currency. La funzione di tali cripto-asset è molto simile a quella della moneta elettronica, come definita all'articolo 2, punto 2, della Direttiva 2009/110/CE del Parlamento europeo e del Consiglio. Come la moneta elettronica, tali cripto-asset sono dei surrogati elettronici di monete e banconote e possono essere utilizzati per effettuare pagamenti"*.

Precisa inoltre il MiCA: "*Di conseguenza, per evitare l'elusione delle norme stabilite nella direttiva 2009/110/CE, qualsiasi definizione di e-money token dovrebbe essere quanto più ampia possibile per comprendere tutti i tipi di cripto-attività che fanno riferimento a un'unica valuta ufficiale* [quella che noi chiamiamo fiat]"

La definizione di EMT dovrebbe essere la più ampia possibile in modo da includere tutti i tipi di cripto-attività che fanno riferimento a una singola valuta ufficiale, comprese le stablecoin.

Gli EMTs sono quindi token usati come mezzo di scambio, ancorati a moneta fiat. Un EMT è token che non è moneta elettronica nel senso tradizionale, ma ha tutte le caratteristiche della moneta elettronica tradizionale.

Nonostante nel MiCA si sia deciso di creare la definizione ETM invece di usare l'ormai diffusissimo termine stablecoin, c'è un (unico) caso dove nel regolamento

si usa il termine stablecoin: quando hanno dovuto fare riferimento alle stablecoin algoritmiche:

"Questo riguarda anche le cosiddette stablecoin algoritmiche che hanno lo scopo di mantenere un valore stabile in relazione a una valuta ufficiale di un paese o a uno o più asset, attraverso protocolli che prevedono l'aumento o la diminuzione dell'offerta di tali cripto-asset in risposta alle variazioni della domanda."

Entropy

Entropia

Livello: intermedio

Argomento: tecnologia

L'entropia nella crittografia, nei bitcoin e nelle criptovalute è un concetto fondamentale, perché ha a che fare con le chiavi private, come vengono generate, e quanto possono essere sicure.

L'entropia utilizzata nella crittografia è l'entropia di Shannon, che fa parte della teoria dell'informazione, e non deve essere confusa con l'entropia della fisica. Nella teoria dell'informazione, l'entropia di una variabile casuale rappresenta il livello medio di "informazione", "sorpresa" o "incertezza" associato ai possibili risultati della variabile stessa. L'unità di misura dell'entropia è il bit, che può assumere solo i valori 0 o 1.

Nella teoria dell'informazione l'entropia di una sorgente di messaggi è l'informazione media contenuta in ogni messaggio emesso. L'entropia di una sorgente risponde a domande come:

- qual è il numero minimo di bit che servono per memorizzare in media un messaggio della sorgente?
- Quanto sono prevedibili i messaggi emessi dalla sorgente?

Per illustrare questo concetto, supponiamo che due persone, Alice e Bob, possano comunicare solo tramite bit, utilizzando un'applicazione per SMS con soli tre pulsanti: "0", "1" e "INVIA". Alice sta osservando un evento casuale che Bob non può vedere e deve comunicare a Bob l'esito dell'evento casuale utilizzando il minor numero possibile di bit. Prima dell'evento, Alice e Bob possono concordare insieme cosa rappresenteranno i bit.

Il primo evento casuale che Alice deve osservare è il lancio di 10 monete in successione, utilizzando una moneta equa. In questo caso, "equa" significa che la moneta non è truccata e quindi la probabilità di ottenere testa è uguale alla probabilità di ottenere croce. Supponiamo che, da ora in poi, tutto sia equo e che non ci siano monete o dadi truccati. Alice e Bob decidono di utilizzare un bit uguale a zero per rappresentare testa e un bit uguale a uno per rappresentare croce. Alice osserva i 10 lanci della moneta, li registra e li invia a Bob: "1101000111". Questa informazione contiene 10 cifre binarie che rappresentano

10 bit di entropia relativi ai 10 eventi casuali, ovvero i 10 lanci della moneta. Le possibili combinazioni di messaggi che Alice avrebbe potuto inviare a Bob sono 2^10, ovvero 1024 combinazioni (2x2x2x2x2x2x2x2x2x2=1024). Alice è stata in grado di esprimere il risultato corretto con soli 10 bit.

Per creare un seed (seme) di 12 parole abbiamo bisogno di 128 bit di informazioni (il livello di sicurezza delle firme ECDSA and Schnorr). Ciò equivale a lanciare una moneta 128 volte e a registrare i risultati come ha fatto Alice per Bob. Come prima, possiamo dedurre che esistono 2128 combinazioni. Si tratta di un numero piuttosto grande, circa 3,4 × 1038 o circa 340.000.000.000.000.000.000.000.000.000.000.000.000.000.

Se vogliamo creare un seed di 24 parole, sono 256 bit di entropia, una quantità così grande che le possibilità di indovinare il seed sono paragonabili alla possibilità di selezionare lo stesso atomo tra tutti gli atomi dell'universo.

L'utilizzo di una passphrase di 24 parole per creare un seed non è necessariamente più sicuro di utilizzarne 12, questo perché le tecniche di crittografia utilizzate (ECDSA e Schnorr) garantiscono una sicurezza a 128 bit, e una passphrase di 12 parole è sufficiente per generare 128 bit di informazioni. Utilizzare una passphrase di 24 parole, anche se può generare una entropia ancora maggiore, non può aumentare la sicurezza a 128 bit di ECDSA e Schnorr, ma aumenta la probabilità di commettere errori nella trascrizione o di dimenticare una delle parole. Quindi, anche se una passphrase più lunga sembra più sicura in teoria, potrebbe in realtà essere meno sicura se ciò porta a errori o problemi di memorizzazione.

Per sfruttare al meglio questa sicurezza, è importante che i valori di entropia provengano da una forte fonte di casualità. Ciò significa lanciare una moneta che non abbia alterazioni, lanciare un dado equo, misurare il rumore, ecc.

NON utilizzate frasi tratte da libri, testi di canzoni, il vostro compleanno o l'indirizzo della vostra strada, la digitazione della tastiera o qualsiasi cosa pensiate sia casuale, perché è molto probabile che non lo sia abbastanza per le esigenze di questo strumento, né tanto meno per mantenere al sicuro i vostri fondi.

I computer, essendo macchine deterministiche, eseguono istruzioni in modo deterministico, dove lo stesso input produce sempre lo stesso output. Questa prevedibilità è fondamentale per la loro affidabilità ma contrasta con il concetto di casualità vera necessaria per produrre una buona entropia.
Un generatore di numeri pseudo-casuali (PRNG) standard utilizza algoritmi matematici che, partendo da un "seme" iniziale, producono una sequenza che appare casuale ma è completamente deterministica e quindi prevedibile se si conosce l'algoritmo e il seme. Per ottenere vera entropia, i computer devono attingere a fonti di casualità esterne al sistema deterministico. Alcune di queste fonti includono:

- **Fenomeni fisici**: rilevazione di rumore termico, decadimento radioattivo,

o fluttuazioni quantistiche
- **Eventi hardware**: timing impreciso tra componenti indipendenti, jitter nell'esecuzione delle istruzioni
- **Input umano**: movimenti del mouse, tempi di battitura sulla tastiera o dei sensori touch
- **Eventi di rete**: timing dei pacchetti, variazioni nel traffico

Sistemi moderni come Linux utilizzano un "entropy pool" che raccoglie dati da queste fonti imprevedibili e li distilla in entropia utilizzabile. Il dispositivo /dev/random, ad esempio, blocca quando l'entropia disponibile è insufficiente.
Per applicazioni critiche per la sicurezza come la crittografia, vengono utilizzati generatori di numeri casuali hardware (TRNG, True Random Number Generators) che sfruttano fenomeni fisici imprevedibili per generare vera casualità.
Un approccio ibrido comune consiste nell'utilizzare una piccola quantità di vera entropia per inizializzare un PRNG, creando così un compromesso tra vera casualità e efficienza computazionale.

ephemeral key

chiave effimera

Livello: avanzato

Argomento: tecnologia

Le chiavi effimere sono chiavi che vengono utilizzate solo per un breve periodo e non vengono conservate dopo l'uso.

Spesso sono derivate per l'uso in una sessione da un'altra chiave che viene conservata a lungo termine. Le chiavi effimere sono utilizzate principalmente nel formato SPHINX Mix e nel routing onion della rete Lightning. Ciò aumenta la sicurezza dei messaggi o dei pagamenti trasportati. Anche se una chiave effimera trapela, solo le informazioni relative a una singola sessione diventano pubbliche.

Epoch

Livello: intermedio

Argomento: tecnologia

Un epoca, o Epoch in inglese, si riferisce generalmente ad una sequenza di blocchi accomunati da uno specifico parametro a seconda del tipo di blockchain o a un periodo di tempo specifico o approssimativo.

Nel caso della blockchain Bitcoin, abbiamo:

- Difficulty epoch che si riferisce alla sequenza di blocchi che hanno la stessa Difficulty

- Halving epoch, è un periodo di tempo di circa 4 anni in cui la ricompensa per i miner viene dimezzata. Questo evento si verifica automaticamente ogni 210.000 blocchi minati

Nel caso delle blockchain che utilizzano la Proof of Stake (PoS), i diversi protocolli PoS hanno modi diversi di definire un'epoca (se la utilizzano).

Le epoche vengono utilizzate per raggiungere i punti di controllo della sicurezza, distribuire le ricompense per le puntate o assegnare un nuovo gruppo di validatori della blockchain.

Ad esempio, un'epoca di Ethereum dura 30.000 blocchi, mentre un'epoca di Cardano dura cinque giorni.

epoch time

Livello: intermedio

Argomento: tecnologia

In informatica, epoch time, o Unix time, è un sistema di misurazione del tempo che fa riferimento al 00:00:00 UTC del 1º gennaio 1970.

In questo sistema, ogni secondo dalla data di riferimento è rappresentato da un numero intero, chiamato timestamp.

Il termine epoch, o epoca, nel caso di Bitcoin si riferisce generalmente ad una sequenza di blocchi accomunati da uno specifico parametro a seconda del tipo di blockchain o a un periodo di tempo specifico o approssimativo.

Il epoch time è spesso espresso come il numero di secondi trascorsi dall'epoch alla data e all'ora attuali. L'epoch più comune utilizzato nei sistemi Unix e Unix-like, nonché in molte altre applicazioni informatiche, è il 1º gennaio 1970 alle 00:00:00 UTC (Coordinated Universal Time). Questa data e ora specifiche sono spesso indicate come "Unix epoch" o "POSIX epoch".

Di conseguenza, quando si parla di epoch time, ci si riferisce al numero di secondi trascorsi da quella data e ora di riferimento. Ad esempio, se il epoch time è di 1609459200 secondi, ciò corrisponde al 1º gennaio 2021 alle 00:00:00 UTC.

L'utilizzo del epoch time è comune nei sistemi informatici per registrare timestamp, calcolare durate e gestire il tempo all'interno dei programmi e dei sistemi operativi. È una rappresentazione semplice e uniforme del tempo che facilita le operazioni di calcolo e confronto delle date e delle ore.

ERC

Acronimo di: Ethereum Request for Comments

Livello: intermedio

Argomento: tecnologia

È utilizzato per indicare delle proposte migliorative per il protocollo Ethereum, analogamente a quanto viene fatto con le BIP di Ethereum.
ERC sono una proposta di standard e convenzioni a livello di applicazione, compresi gli standard di smart contract come i token fungibili (ERC20), i registri dei nomi (ERC26, ERC137), gli schemi URI (ERC67), i formati delle librerie/pacchetti (EIP82) e i formati dei portafogli (EIP75, EIP85).

ERC-1155

Livello: intermedio

Argomento: tecnologia

Una proposta del 2018 che introduce uno standard per l'implementazione e gestione Multi Token all'interno dello stesso smart contract di token fungibili, token non fungibili o altre configurazioni (ad es. token semi fungibili), e in modo più efficiente rispetto ai precedenti standard ERC-20 e ERC-721.

ERC-20

Livello: intermedio

Argomento: tecnologia

È il primo standard Ethereum per la creazione di smart contract per la generazione e gestione dei token (ERC-20). ERC-20 definisce un elenco comune di regole e interfacce per lo smart contract, semplificando il lavoro degli sviluppatori e consentendo la realizzazione di strumenti, ad esempio wallet, che possano gestire i token di questi smart contract. E' il protocollo più usato per la creazione di token e le conseguenti ICO.

ERC-2981 NFT Royalty Standard

Livello: avanzato

Argomento: tecnologia

È uno standard per i smart contract su blockchain Ethereum per impostare le informazioni sul pagamento delle royalty per gli NFT per i marketplace NFT e i partecipanti all'ecosistema

ERC-721

Livello: intermedio

Argomento: tecnologia

È uno standard per la blockchain Ethereum per la creazione di smart contract i cui token, rispetto all'ERC-20, hanno la proprietà di essere NFT, ovvero non fungibili.

Erlay

Livello: avanzato

Argomento: tecnologia

Erlay è una modifica al transaction relay protocol, il protocollo di trasmissione delle transazioni, a livello peer-to-peer, dove i full node comunicano e condividono i dati sulle transazioni trasmesse alla rete.

La modifica apporterebbe un notevole guadagno in termini di efficienza della larghezza di banda a questo livello peer-to-peer, rendendo più facile per un maggior numero di persone gestire i full node, in particolare per coloro che vivono in aree con una connettività Internet insufficiente.

Una importante svolta nell'ingegneria delle reti distribuite che consentirà a Bitcoin di diventare una rete più robusta, affidabile e privata: più robusta perché consente a un maggior numero di individui di partecipare alla convalida della rete, abbassando la barriera all'ingresso con la diminuzione della larghezza di banda di Internet in modo che le persone possano gestire più facilmente un full node; più affidabile aumentando la connettività tra i nodi; e più privata rendendo più difficile per gli aggressori identificare il nodo da cui proviene una transazione.

Nel protocollo Gossip attualmente in uso su Bitcoin, la maggior parte dei full node è configurata per pubblicizzare ogni nuova transazione a tutti i loro peer, a meno che non abbiano precedentemente ricevuto un annuncio sulla transazione da quel peer. Con un minimo di 32 byte per txid pubblicizzato e nodi che hanno un massimo predefinito di 125 peer, questo consuma una grande quantità di larghezza di banda ridondante, dato che ogni nodo deve venire a conoscenza di una transazione solo da uno dei suoi peer.

Erlay è una proposta divisa in due parti che, in primo luogo, limita il numero di peer a cui un nodo pubblicizza direttamente le transazioni (default: 8) e, in secondo luogo, utilizza la riconciliazione dei set basata su libminisketch con il resto dei suoi peer per evitare di inviare il txid di qualsiasi transazione che il peer ricevente ha già visto.

Erlay si adatta a un numero maggiore di peer molto meglio del protocollo attuale, rendendo pratico per i nodi accettare più connessioni di quante ne accettino ora. Questo migliorerebbe la robustezza della rete di relay contro le partizioni della rete, sia accidentali che intenzionali.

Escrow

Acconto di garanzia

Livello: intermedio

Argomento: economia

Un escrow è un servizio che viene utilizzato per facilitare transazioni tra due parti. In una transazione con un escrow, una terza parte (l'escrow agent) trattiene temporaneamente i fondi o le proprietà in questione fino a quando le condizioni dell'accordo non sono state soddisfatte da entrambe le parti.

Ad esempio, se due parti stanno vendendo e acquistando un bene di valore, come una casa, possono utilizzare un servizio di escrow per garantire che il denaro e il titolo di proprietà siano protetti durante il processo di transazione.

Il processo di escrow funziona generalmente in questo modo: le parti concordano sui termini dell'accordo, inclusi il prezzo di acquisto e le condizioni di consegna. Quindi, depositano i fondi o la proprietà in questione presso l'escrow agent. Una volta che le condizioni dell'accordo sono state soddisfatte, l'escrow agent rilascia i fondi o la proprietà alle parti coinvolte.

In questo modo, l'escrow offre una maggiore sicurezza e protezione per entrambe le parti coinvolte nella transazione, riducendo al minimo il rischio di frode o disaccordo.

Si tratta quindi di una terza parte affidabile che svolge la funzione di arbitro imparziale nell'ambito di una transazione. Questa terza parte gestisce un accordo tra due parti, nel quale somme di denaro o titoli di proprietà oggetto del contratto vengono depositati presso di essa a titolo di garanzia. Questi fondi saranno poi rilasciati all'avveramento di determinate condizioni stabilite dalle parti.

Bitcoin Script può essere utilizzato per creare un semplice escrow utilizzando opcode multi-firma.

ESMA

Acronimo di: European Securities and Markets Authority

Autorità europea degli strumenti finanziari e dei mercati

Livello: intermedio

Argomento: politica

L'ESMA è l'Autorità europea degli strumenti finanziari e dei mercati indipendente nell'UE, fondata nel 2011.

L'accordo provvisorio sul MiCA prevede che i CASP necessitino di autorizzazione per operare nell'UE, con i CASPS più grossi che saranno monitorati dall'ESMA.

etching

incidere

Livello: intermedio

Argomento: tecnologia

In relazione a Bitcoin, il termine “etching”, in italiano incidere, viene utilizzato nel contesto dei Runes, un nuovo standard per token fungibili sulla blockchain di Bitcoin.

L’etching è il processo fondamentale nella creazione di un Rune, dove il token digitale viene inizialmente creato e definito sulla blockchain.

Più precisamente, l’etching comporta:

- Definizione delle proprietà del Rune: Si stabiliscono le caratteristiche fondamentali del token, come il nome, il simbolo e la fornitura totale.
- Creazione di un’Inscription sulla blockchain: Vengono registrati i dati del Rune sulla blockchain di Bitcoin, creando un’impronta digitale unica e immutabile.
- Associazione di un numero di serie unico a ciascun Rune: Ogni Rune riceve un identificatore univoco che lo distingue da tutti gli altri token.

L’etching rappresenta il primo passo nel ciclo di vita di un Rune. Successivamente, il Rune può essere sottoposto a minting, ovvero il processo di generazione di nuovi token. Il minting può essere strutturato come un sistema aperto o chiuso, definito da specifiche condizioni preimpostate durante la fase di etching.

L’utilizzo del termine “etching” sottolinea la natura indelebile e permanente del processo di creazione di un Rune. Una volta etched, un Rune esiste in modo permanente sulla blockchain di Bitcoin e le sue proprietà non possono essere modificate.

ETF

Acronimo di: exchange traded fund

Livello: intermedio

Argomento: finanza

Gli ETF, exchange-traded fund in italiano fondo scambiato in borsa, sono un tipo di fondi d’investimento quotati in borsa allo stesso modo di un normale titolo, che seguono un indice, un settore, una merce o un altro asset e più recentemente anche criptovalute.

Un ETF Bitcoin è un fondo negoziato in borsa (ETF) che investe in Bitcoin. Gli ETF sono un tipo di investimento che segue un indice di mercato, come l’indice S&P 500. In questo caso, l’indice è il prezzo di Bitcoin.

Gli ETF Bitcoin sono un modo per investire in Bitcoin senza dover acquistare e custodire effettivamente Bitcoin. Ciò può essere utile per gli investitori che non vogliono o non possono acquistare Bitcoin direttamente.

Gli ETF Bitcoin sono ancora relativamente nuovi e non sono disponibili in tutti i paesi. Tuttavia, sono in aumento di popolarità e sono visti come un modo per

rendere più accessibili gli investimenti in Bitcoin, e per qualcuno spingere verso l'alto il prezzo di Bitcoin.

Negli Stati Uniti la SEC ha approvato i primi ETF Spot il 10 Gennaio 2024.

ETF Spot Bitcoin Un ETF Spot Bitcoin è un fondo comune di investimento aperto che può emettere o rimborsare quote in base alla domanda.
È progettato per seguire da vicino il prezzo attuale del Bitcoin. Un ETF viene negoziato su importanti borse, simile alle azioni, e può essere acquistato e venduto durante l'intera giornata di negoziazione a prezzi in linea con l'asset sottostante in questo caso Bitcoin.
Gli ETF consentono la creazione e il rimborso di quote per soddisfare la domanda. Se il prezzo dell'ETF si discosta dal valore dell'asset sottostante, i partecipanti autorizzati possono sfruttare opportunità di arbitraggio. Questo meccanismo aiuta a mantenere il prezzo dell'ETF allineato con il NAV (net asset value, valore) dell'asset sottostante.

ETH

Acronimo di: Ether

Livello: base

Argomento: tecnologia

Unità di conto della blockchain Ethereum che funge quindi sia da criptovaluta, sia da carburante (vedi Gas price)

Ethereum

Livello: base

Argomento: tecnologia

Ethereum è una piattaforma decentralizzata basata su blockchain che consente la creazione e l'esecuzione di contratti intelligenti (smart contracts) Turing-completi.
È la seconda criptovaluta più grande al mondo per capitalizzazione di mercato, dopo Bitcoin.

Ethereum è una piattaforma open source. La blockchain di Ethereum è passata ad un consenso proof-of-stake, rispetto al consenso proof-of-work utilizzato da Bitcoin che utilizzava inizialmente anche Ethereum.

Ethereum è una piattaforma versatile che può essere utilizzata per una varietà di applicazioni, tra cui:

- Finanza decentralizzata DeFi: Ethereum è la piattaforma su cui si basa la maggior parte delle applicazioni DeFi, che offrono servizi finanziari come

prestiti, investimenti e scambi senza la necessità di intermediari centralizzati. Tuttavia, la DeFi su Ethereum è stata oggetto di attacchi hacker, che hanno portato a perdite di milioni di dollari.
- Giochi: Ethereum può essere utilizzato per creare giochi online che sono più coinvolgenti e interattivi grazie alla possibilità di implementare contratti intelligenti. Tuttavia, la creazione di giochi su Ethereum è costosa e richiede competenze tecniche avanzate.
- Arte: Ethereum può essere utilizzato per creare opere d'arte digitali che sono protette da contraffazione grazie alla tecnologia blockchain.

Bitcoin è la criptovaluta più grande al mondo per capitalizzazione di mercato. È stata progettata per essere un mezzo di pagamento digitale peer-to-peer, e non ha le stesse ambizioni di Ethereum in termini di applicazioni.

Bitcoin ha una serie di vantaggi rispetto a Ethereum, tra cui:

- Maggiore sicurezza: Bitcoin è basato su un consenso proof-of-work, che è più sicuro rispetto al consenso proof-of-stake utilizzato da Ethereum.
- Maggiore stabilità: Bitcoin ha una storia più lunga e consolidata di Ethereum, e la sua volatilità è inferiore.
- Maggiore accettazione: Bitcoin è accettato da un numero maggiore di aziende e individui rispetto a Ethereum.

In conclusione, Ethereum è una piattaforma versatile con un potenziale significativo, ma Bitcoin ha una serie di vantaggi che lo rendono la criptovaluta più sicura, stabile e accettata al mondo.

EVM

Acronimo di: Ethereum Virtual Machine

Livello: avanzato

Argomento: tecnologia

L'Ethereum Virtual Machine (EVM) è un computer virtuale o macchina virtuale che esegue smart contract sulla blockchain di Ethereum.
È un ambiente di esecuzione sandboxed che isola gli smart contract l'uno dall'altro e dal resto del sistema. L'EVM è implementato in tutti i nodi della rete Ethereum, il che significa che tutti gli smart contract vengono eseguiti in modo identico su tutti i nodi.

L'EVM è stato progettato per essere semplice e efficiente, pur essendo abbastanza potente da eseguire una varietà di applicazioni complesse. L'EVM ha set di istruzioni limitato, ma ciò consente di ottimizzarne l'implementazione.

Gli smart contract vengono compilati in bytecode EVM prima di essere distribuiti sulla blockchain di Ethereum. Il bytecode EVM è un codice macchina che può essere eseguito dall'EVM. Quando uno smart contract viene eseguito, l'EVM legge il bytecode e lo esegue passo dopo passo.

L'EVM è una parte essenziale dell'ecosistema Ethereum. Consente agli sviluppatori di creare e distribuire smart contract che possono essere utilizzati per una varietà di scopi, come DApp o applicazioni decentralizzate, DeFi o finanza decentralizzata ()e creazione di token fungibili e NFT o token non fungibili.

L'EVM è implementato in tutti i nodi della rete Ethereum, il che significa che gli smart contract vengono eseguiti in modo identico su tutti i nodi. Ciò garantisce la decentralizzazione della rete Ethereum.

Il successo e la quantità di sviluppi effettuati su l'EVM ha fatto in modo che siano nate diverse blockchain che implementano EVM compatibili con quella Ethereum.

Exchange

Livello: base

Argomento: finanza

Gli exchange di criptovalute sono piattaforme digitali che consentono agli utenti di acquistare, vendere e scambiare bitcoin e criptovalute. Sono simili alle borse valori tradizionali, ma si concentrano sulle criptovalute invece delle valute fiat.

Esistono due tipi principali di exchange di criptovalute:

- CEX o centralizzati
- DEX o decentralizzati

Gli Exchange offrono una serie di funzionalità, tra cui:

- Acquisto e vendita di criptovalute con valute fiat
- Scambio di criptovalute tra loro
- Depositi e prelievi di criptovalute
- Strumenti di trading avanzati

L'exchange è solito trattenere una parte degli scambi come fee (tassa di transazione): è un vero e proprio sistema digitale di cambio valute e funziona in modo simile a quelli tradizionali.

Il primo exchange Bitcoin è stato New Liberty Standard, che ha stabilito il tasso di cambio iniziale di Bitcoin di 1.309,03 Bitcoin per $1.

Executive Order 6102

Ordine esecutivo 6102

Livello: intermedio

Argomento: politica

L'ordine esecutivo 6102 viene a volte citato come esempio per illustrare il potenziale rischio di confisca o restrizione da parte del governo delle risorse finanziarie

dei cittadini.

L'ordine esecutivo 6102 è stato emesso dal presidente degli Stati Uniti Franklin D. Roosevelt nel 1933 durante la Grande depressione per proibire la detenzione di oro da parte dei cittadini statunitensi. L'ordine esecutivo stabiliva che tutto l'oro in possesso dei cittadini statunitensi doveva essere consegnato alle banche federali entro un certo periodo di tempo, a un prezzo stabilito dal governo. In cambio, i cittadini ricevevano una quantità equivalente di dollari in contanti.

È possibile che un governo possa emettere un ordine esecutivo o una legislazione che restringa o proibisca l'uso dei Bitcoin o di altre criptovalute all'interno dei propri confini. In effetti, alcuni paesi hanno già adottato misure di questo tipo per limitare l'utilizzo delle criptovalute. Ad esempio, il governo cinese ha vietato l'utilizzo delle criptovalute come mezzo di pagamento nel paese e ha bloccato l'accesso ai principali exchange di criptovalute. Altri paesi, come il Bangladesh e l'Iran, hanno emesso divieti simili.

Tuttavia, è importante notare che le criptovalute come i Bitcoin sono difficili da tracciare e da censurare, sono basate sulla tecnologia p2p, decentralizzata e non dipende da un singolo ente o autorità centrale. Sono digitali e non esistono come entità fisica e l'uso della blockchain fa in modo che un utente possa avere il controllo dei propri bitcoin senza doverli memorizzare fisicamente su un device o un supporto fisico. Ad esempio anche gli hardware wallet di fatto non contengono al loro interno i Bitcoin, ma solo le chiavi private per firmare le transazioni e per trasferire i bitcoin, e la perdita dell'harware wallet non comporta la perdita dei propri fondi se l'utente ha effettuato un backup del seed delle proprie chiavi.

Ciò significa che anche se un governo proibisce l'uso delle criptovalute, potrebbe essere difficile per esso impedirne detenzione e utilizzo all'interno dei propri confini.

Inoltre, poiché le criptovalute sono globali e non dipendono da una singola giurisdizione, un ordine esecutivo o una legislazione di un singolo paese potrebbero non avere un impatto significativo sull'utilizzo delle criptovalute a livello globale.

extended key

chiave estesa

Livello: intermedio

Argomento: tecnologia

Una extended key, chiave estesa, è una chiave privata o una chiave pubblica che può essere utilizzata per ricavare nuove chiavi in un Wallet HD, gerarchico deterministico.

Pertanto, è possibile avere una singola chiave privata estesa e utilizzarla come fonte per tutte le chiavi private e pubbliche figlie del proprio wallet. Inoltre, una chiave pubblica estesa corrispondente genererà le stesse chiavi pubbliche figlie.

ExtraNonce

Livello: avanzato

Argomento: tecnologia

I miner bitcoin incrementano il nonce nel tentativo di creare un blocco valido con un valore hash che soddisfi un determinato obiettivo di difficoltà. Bitcoin memorizza il nonce nel campo extraNonce che fa parte della transazione coinbase, memorizzata come il nodo più a sinistra dell'albero di Merkle; il campo ExtraNonce, che si trova nella transazione coinbase, si incrementa ogni volta che il campo nonce si esaurisce, ovvero che lo spazio di ricerca è esaurito. Poiché il campo nonce è lungo 32 bit e l'obiettivo iniziale di difficoltà di Bitcoin richiedeva una scansione media di 32 bit, il nonce a volte, ma non sempre, andava in overflow.

L'ExtraNonce funziona come un "contatore libero", senza azzerarsi tra i blocchi estratti. La velocità con cui un determinato miner incrementa l'ExtraNonce è molto più veloce di quanto indicherebbe il suo hashrate effettivo, in base al codice sorgente originale di Bitcoin. Ogni pochi secondi durante il mining, viene controllato il blocco migliore. Se il blocco migliore cambia, l'ExtraNonce viene incrementato ulteriormente. Normalmente ogni blocco esterno ricevuto incrementa l'ExtraNonce, ad eccezione di un insieme di primi blocchi che si ipotizza siano stati minati da Satoshi Nakamoto, che non sembrano seguire questa regola.

FA

Acronimo di: Fundamental Analysis

Analisi Fondamentale

Livello: avanzato

Argomento: finanza

L'analisi fondamentale nonostante sia tradizionalmente utilizzata per valutare le azioni, è applicabile a quasi tutti i tipi di attività, comprese le criptovalute. E' un metodo utilizzato da investitori e trader nei mercati finanziari per valutare il valore intrinseco di un'attività esaminando il maggior numero di fattori qualitativi e quantitativi possibili, come la gestione e la reputazione dell'azienda, la salute del settore, la capitalizzazione di mercato, e altri fattori economici. L'obiettivo dell'analisi fondamentale è determinare se il prezzo di un'attività è sopravvalutato o sottovalutato. L'analisi fondamentale funziona sulla comprensione del fatto che il potenziale futuro di un bene dovrebbe essere basato su qualcosa di più della semplice performance precedente. Tiene conto delle condizioni sia microeconomiche che macroeconomiche che possono avere un effetto su quel particolare mercato. Pertanto, possiamo considerare che l'analisi fondamentale cerchi di determinare come i fattori esterni possano influenzare le

prestazioni di un'azienda o di un progetto, in particolare di quei fattori che non sono immediatamente evidenti. Queste considerazioni si concentrano su aspetti meno tangibili e più qualitativi, come la leadership di un'azienda e il comportamento di quei leader in altre iniziative imprenditoriali in passato. L'analisi fondamentale cerca anche di comprendere meglio il mercato specifico del settore e il potenziale futuro di un prodotto o servizio in quel mercato. In definitiva, il suo obiettivo è trovare un prezzo quantitativo che possa essere confrontato con il prezzo effettivo del rispettivo asset. L'analisi fondamentale è quindi un metodo che può aiutare a determinare se il prezzo valutato è troppo alto o troppo basso.

Fan Token

Livello: intermedio

Argomento: finanza

è un token creato e collegato a un club sportivo.

Generalmente è un utility token poiché garantisce al suo possessore alcuni vantaggi, permette ai detentori l'accesso di beni e servizi, ad esempio, il titolare del token può avere potere decisionale in alcune questioni aziendali, come il voto sul futuro kit della prima squadra, sconti sui prodotti del club, esclusività in certi eventi, promozioni e accesso prioritario per acquistare biglietti per le partite; in alcuni casi, inoltre, possono influenzare la gestione della squadra. Una delle principali emittenti di questi prodotti è Chiliz che ha sviluppato la piattaforma Socios.com, che utilizza il token CHZ creato su blockchain Ethereum.
Altra emittente è Bitci, la criptobanca turca che ha creato la criptovaluta della nazionale di calcio spagnola (SNFT) e quelle di altri club di LaLiga

FASB

Acronimo di: Financial Accounting Standards Board

Livello: intermedio

Argomento: politica

Il Financial Accounting Standards Board (FASB) è un ente privato di normazione il cui scopo principale è stabilire e migliorare i Principi Contabili Generalmente Accettati (Generally Accepted Accounting Principles, GAAP) negli Stati Uniti nell'interesse pubblico.

La SEC ha designato il FASB come l'organizzazione responsabile per la definizione degli standard contabili per le società quotate negli Stati Uniti.
Il FASB ha sostituito l'Accounting Principles Board (APB) dell'American Institute of Certified Public Accountants (AICPA) il 1º luglio 1973.
Il FASB è gestito dalla Fondazione per la Contabilità Finanziaria, un'organizzazione non a scopo di lucro.

Gli standard contabili del FASB sono riconosciuti come autorevoli da molte organizzazioni, tra cui le Commissioni per l'Amministrazione della Contabilità a livello statale e l'American Institute of CPAs (AICPA).

FATF

Acronimo di: Financial Action Task Force

GAFI Gruppo d'azione finanziaria

Livello: intermedio

Argomento: politica

La FATF, Financial Action Task Force, conosciuta anche con il suo nome francese GAFI (Groupe d'action financière), è un'organizzazione intergovernativa fondata nel 1989 su iniziativa del G7 per sviluppare politiche di lotta al riciclaggio di denaro.

Nel 2001, il suo mandato è stato ampliato per includere la lotta al finanziamento del terrorismo. Nel 2019 la FATF ha introdotto nuovi regolamenti rigorosi, in particolare la FATF Travel Rule, per i VASP che devono essere implementati dalla sua rete di oltre 200 membri, che include l'Unione europea.

La FATF vuole essere il controllore globale contro il riciclaggio di denaro e il finanziamento del terrorismo. L'organismo intergovernativo stabilisce degli standard internazionali che mirano a prevenire queste attività illegali. In qualità di organo decisionale, il FATF lavora per generare la volontà politica necessaria a portare avanti riforme legislative e normative nazionali in questi settori.

Con più di 200 paesi e giurisdizioni impegnati ad attuarle, il FATF ha sviluppato le raccomandazioni del FATF, o standard del FATF, con l'obbiettivo di fornire una risposta globale coordinata per prevenire il crimine organizzato, la corruzione e il terrorismo. Aiutano le autorità a perseguire il denaro dei criminali che trafficano in droghe illegali, traffico di esseri umani e altri crimini. Il FATF lavora anche per fermare il finanziamento delle armi di distruzione di massa.

Il FATF esamina le tecniche di riciclaggio di denaro e di finanziamento del terrorismo e rafforza continuamente i suoi standard per affrontare nuovi rischi, come la regolamentazione dei beni virtuali, che si sono diffusi con l'aumento della popolarità delle criptovalute. Il FATF monitora i paesi per assicurare che attuino pienamente ed efficacemente gli standard del FATF, e tiene in considerazione i paesi che non li rispettano.

Faucet

Livello: avanzato

Argomento: tecnologia

È un sistema di ricompensa in criptovaluta di solito su un sito Web o un'app, che distribuisce in modo gratuito o premia gli utenti per il completamento di determinati compiti. È una tecnica usata a volte quando si lancia un altcoin per attirare la gente alla moneta.

Il primo Faucet bitcoin è stato sviluppato da Gavin Andresen nel 2010, e inizialmente distribuiva cinque bitcoin a persona.

FDIC

Acronimo di: United States Federal Deposit Insurance Corporation

Livello: intermedio

Argomento: politica

La Federal Deposit Insurance Corporation (FDIC) è un'agenzia indipendente che esiste per convincere il pubblico che i conti di deposito assicurati dalla FDIC siano una riserva di valore sicura. L'importo standard dell'assicurazione FDIC è di 250.000 dollari per depositante, per banca, per ogni categoria di proprietà del conto.

Se la FDIC sia in grado di coprire tutti i depositanti che pretende di assicurare è molto discusso. Alcuni rapporti sostengono che la FDIC può permettersi di coprire solo i conti di deposito di alcune delle banche più grandi.

Durante la Grande Depressione, le banche fallirono. I mutuatari non riuscirono a rispettare i prestiti per gli investimenti a margine, i mutui e altre linee di credito. Le attività bancarie erano scese al di sotto delle passività per molti anni e le banche non erano più in grado di adempiere ai loro doveri fiduciari. L'esaurimento della liquidità insieme al panico diffuso causò corse agli sportelli e la frustrazione dei consumatori per l'instabilità delle banche centrali.

L'assicurazione FDIC è stata avviata nel 1934 per ripristinare la fiducia nonostante le vulnerabilità di un sistema bancario centralizzato. Da allora, nessun conto FDIC ha perso i fondi assicurati a causa del fallimento di una banca. Il denaro dei contribuenti non finanzia la FDIC. Invece, le banche e gli istituti di risparmio pagano un premio assicurativo per diventare membri della FDIC. Le entità più rischiose pagano un premio più alto al fondo.

La FDIC deve mantenere la liquidità in una riserva contingente per coprire i probabili fallimenti dei conti per un periodo di 12 mesi. La FDIC può generare flussi di cassa vendendo le attività delle banche fallite, applicando commissioni speciali e anticipando i premi. In teoria, le riserve contingenti a 12 mesi e la liquidità facilmente accessibile significano che anche quando la FDIC ha un bilancio negativo, può comunque proteggere i conti di deposito.

A seguito di un ordine del tribunale di giugno 2024 la FDIC è stata costretta a rendere pubbliche le lettere relative a quella che è stata definita come Operation

Choke Point 2.0, con le quali l'FDIC sconsigliava alle banche di impegnarsi in qualsiasi attività legata alle criptovalute.

Fed

Acronimo di: Federal Reserve

Livello: intermedio

Argomento: politica

La Federal Reserve, o Federal Reserve System, o semplicemente la Fed, è la banca centrale degli Stati Uniti d'America. In italiano è traducibile come Riserva Federale, anche se viene comunemente utilizzato il termine inglese anche in Italia. La Fed è un sistema bancario centrale privato che agisce come agente monetario del governo statunitense; supervisiona le banche membri, regola i mercati dei capitali e fissa il coefficiente di riserva.

Il Congresso originariamente intendeva che la banca centrale rimanesse isolata dal governo federale e dall'influenza politica, ma nel tempo la Fed e il Tesoro hanno iniziato a collaborare strettamente sulla spesa pubblica e sulla politica monetaria. La Fed non stampa fisicamente denaro, ma emette credito digitalmente alle banche commerciali membri. Poiché la Fed non ha tecnicamente l'autorità per spendere, può solo aumentare l'offerta di moneta prestando denaro e creando così nuove riserve per le banche commerciali.

La Fed può finanziare un progetto del Congresso acquistando titoli del Tesoro del governo, creando nuovi conti di riserva e rimettendo i pagamenti degli interessi al Tesoro degli Stati Uniti. Di conseguenza, il governo può prendere in prestito essenzialmente senza alcun costo di capitale.

Federated Blockchain

Livello: avanzato

Argomento: tecnologia

una blockchain consortile, detta anche blockchain federata, è una blockchain abbastanza simile a una blockchain privata nella quale sono ammessi ad entrare solo partecipanti preselezionati. Inoltre, tutti i partecipanti hanno un uguale potere, e quindi è questo il tipo che viene utilizzato per costruire un meccanismo di consenso tra le operazioni. Infine, poiché i partecipanti sono preselezionati, non è necessaria una criptovaluta per evitare spam o creare incentivi alla partecipazione.

Fedimint

Livello: avanzato

Argomento: tecnologia

Fedimint è un protocollo open source per custodire e transare bitcoin in un contesto di community, costruito su una solida base di privacy.

Fedimint nasce come alternativa rispetto ai sistemi Custodial di terze parti. Fedimint è un meccanismo che consente ai Bitcoiner e ai membri fidati della comunità di far entrare le loro comunità locali in Bitcoin in un modo più responsabile e privato.

Idealmente, i bitcoiner dovrebbero gestire i propri nodi e custodire i propri fondi e le proprie chiavi private.

Molte persone trovano proibitive le sfide tecniche di gestire i propri nodi e di custodire i propri fondi attraverso la gestione della frase di recupero, e scelgono di affidarsi a un depositario terzo come gli exchange o i wallet custodial.

Questi utenti sacrificano la loro privacy e sicurezza a favore della velocità e della convenienza. Questo rappresenta un rischio sistemico per la rete bitcoin, poiché grandi quantità di bitcoin sono aggregate in singoli depositari.

Fedimint si propone di risolvere questo problema distribuendo la custodia in milioni di comunità, rendendo semplice essere la banca di sé stessi. Queste "banche" comunitarie sono note come Fedimint Federations.

Fedimint permette ai bitcoiner di coinvolgere nuovi utenti, assistendoli nel loro modello di custodia e pagamento. Invece di indirizzare un nuovo bitcoiner a un depositario terzo, è possibile effettuare l'onboarding in prima persona come parte di una Federazione.

In altre parole, potete essere la banca di vostra madre, dei vostri amici o dei vostri villaggi.

Queste relazioni strette e di fiducia sono chiamate "custodi di seconda parte". I custodi della federazione Fedimint dovrebbero essere amici intimi e membri della famiglia che si conosce personalmente e che si può avere un rapporto diretto nel caso in cui tentino di violare la vostra fiducia.

Questo fornisce ai bitcoiner una terza opzione tra i custodi centralizzati di terze parti e l'autocustodia.

Fedimint è interoperabile con Lightning Network. Gli utenti di Fedimint possono in qualsiasi momento spostare i propri fondi nel proprio lightning wallet in autocustodia.

Questo permette agli utenti Fedimint di rimanere parte della più ampia rete Lightning, rendendo possibile il pagamento di commercianti, di altri utenti o anche il passaggio da un Fedimint all'altro.

In questo modo, un utente che in precedenza utilizzava un depositario di terze parti per comodità può mantenere tale comodità, migliorando al contempo la propria privacy e il controllo delle proprie finanze.

C'è un compromesso in questo caso, poiché si sta affidando il proprio bitcoin a una federazione. Per questo motivo sarà importante "conoscere la propria federazione".

A settembre 2023 è stata rilasciata la v0.1.0, prima release ufficiale.

Fee

Commissione

Livello: base

Argomento: tecnologia

Con questo termine nel caso delle criptovalute ci si riferisce ad una commissione che viene pagata per effettuare una transazione.

Fee per le transazioni on-chain Le transazioni on chain sono quelle che vengono confermate all'interno di un blocco della blockchain bitcoin.
Per queste, è l'utente che crea la transazione che decide quale importo vuole pagare per inserire la sua transazione on-chain. La fee viene incassata dal miner che inserisce la transazione nel blocco da lui minato, e costituisce quindi un incentivo ai miner per validare la transazione inserendola nel blocco della blockchain.

Le fee per confermare velocemente on-chain una transazione possono variare dal corrispondente di pochi centesimi a centinaia di dollari, a seconda dei livelli di congestione della mempool, l'area di transito delle transazioni in attesa di essere confermate, e delle dimensioni della transazione. Le commissioni di transazione sono espresse in satoshi per unità di dati, abbreviato in sats/vByte.

Il protocollo bitcoin non definisce una fee di base obbligatoria, ma la maggior parte dei nodi della rete non trasmetterà le transazioni con una tariffa inferiore alla minRelayTxFee, generalmente 1 satoshi per vByte.
Inoltre, la maggior parte dei miner non include le transazioni al di sotto della *minRelayTxFee* nei propri blocchi.

Molti wallet software possono avere impostate delle regole per impostare le fee, ad esempio delle soglie minime.

La tariffa minima necessaria per la conferma di una transazione varia nel tempo e deriva dall'intersezione della domanda e dell'offerta nel libero mercato dei blocchi della blockchain Bitcoin. Per quanto riguarda la dimensione dell'offerta, Bitcoin ha una block size, la dimensione massima del blocco (attualmente un milione di vbyte) che limita la quantità massima di dati di transazione che possono essere aggiunti a un blocco.

Le fee on-chain non sono condizionate dall'importo della transazione, ovvero non è necessario pagare fee più alte se l'importo della transazione è più alto, ma possono essere condizionate dal peso ovvero dalla dimensione della transazione; per il miner, che può decidere in base alle fee quali transazioni inserire nel

blocco che sta minando, è assolutamente ininfluente l'importo della transazione; è invece importante quale sia il peso della transazione ovvero lo spazio che la transazione occupa nel blocco.
Una transazione che ha molti input in ingresso e molti output in uscita, sarà ad esempio più pesante rispetto ad una transazione che ha un solo input in ingresso e uno o due in uscita, a prescindere dagli importi in bitcoin delle transazioni, e quindi per essere confermata prima diventa opportuno attribuirgli delle fee più alte.

I miner nel confezionare un blocco (block template) scelgono dalla mempool quelle transazioni che gli consentono di massimizzare il MEV, miner extractable value o maximal extractable value; se la mempool è particolarmente congestionata, ovvero ci sono molte transazioni in attesa, diventa necessario impostare fee più alte per vedere la propria transazione confermata.

Una volta creata una transazione e trasmessa alla rete, se la transazione tarda ad essere confermata, esistono delle tecniche che possono velocizzare la conferma quali RBF, Replace By Fee che aumenta l'importo delle fee, o CPFP.

Fee su Lightning Network Nel contesto Lightning Network, sono i nodi che gestiscono i canali attraverso i quali passano i pagamenti, i routing node, che addebitano le commissioni di instradamento per l'inoltro dei pagamenti di altri utenti.

Bisogna anche considerare che un pagamento su Lightning Network può attraversare diversi canali: sia perché non è detto che esista un canale che collega direttamente il nodo al quale è collegato chi paga, e chi riceve, e anche perché i canali possono non avere sufficiente liquidità e quindi può essere necessario frazionare il pagamento su diversi canali. Questo fa in modo che le fee totali saranno uguali alla somma delle fee dei singoli canali. I routing node possono addebitare una commissione per il ruolo di intermediario, anche se non sono obbligati a farlo e possono scegliere di instradare i pagamenti gratuitamente.

I singoli nodi possono stabilire le proprie politiche tariffarie, che possono farlo sulla base del calcolo come somma di una tariffa di base **base_fee** fissa e di una tariffa **fee_rate** dipendente dall'importo del pagamento.

base_fee La base_fee è una somma fissa che viene addebitata per ogni inoltro, in genere 1 satoshi. È anche possibile impostare una tariffa base più alta o pari a 0, o addebitare qualsiasi importo di millisatoshi. Poiché ogni inoltro costa in termini di potenza di calcolo e di memoria, la base_fee ha lo scopo di compensare gli sforzi compiuti per inoltrare un pagamento.

Ad esempio, per ogni nuovo stato del canale il nodo deve tenere in archivio una nuova chiave di revoca. Se si utilizza una watchtower, queste informazioni devono essere inviate e memorizzate anche sulla watchtower.

Tali informazioni devono essere conservate fino alla chiusura del canale, il che può essere costoso.

Per migliorare le prestazioni di Lightning Network esiste una iniziativa chiamata Zero Base Fee

fee_rate Il fee_rate è una percentuale del pagamento che viene inoltrato, generalmente misurata in ppm, parti per milione. Ha lo scopo di compensare il capitale impegnato nei canali Lightning.

Fee negli exchange Nel caso degli exchange, la fee può essere un importo proporzionale impostato dall'exchange per effettuare lo scambio.

fee bumping

Livello: avanzato

Argomento: tecnologia

Il fee bumping su Bitcoin è una tecnica che consente di aumentare la priorità di una transazione nella rete Bitcoin, in modo che venga confermata più rapidamente, aumentando le fee che il miner guadagnerebbe confermando quella transazione.

La fee richiesta per la conferma rapida di una transazione varia a seconda delle condizioni della rete.

In genere oscilla lentamente, ma a volte aumenta a causa di transazioni spam o di una serie di blocchi casualmente lenti. In questi casi, è possibile che le transazioni in entrata o in uscita rimangano bloccate in uno stato di non conferma per molto tempo. I wallet dovrebbero evitare questo problema nel 99% dei casi prevedendo con precisione una fee appropriata e dovrebbero essere in grado di ridurre gradualmente le fee nel restante 1% dei casi, ma in generale le fee sono gestite piuttosto male dai wallet attuali.

Ci sono alcuni modi su come aumentare la fee su una transazione bloccata nella mempool in attesa di conferma. Questo avviene sempre creando una nuova transazione che spenderà le monete inviate dalla transazione bloccata chiamata CPFP child-pays-for-parent, o sostituirà la transazione bloccata tramite RBF replace-by-fee. Le istruzioni variano in modo significativo a seconda del software del wallet.

Fee sniping

Livello: avanzato

Argomento: tecnologia

Il Fee sniping si verifica quando un miner deliberatamente ri-mina uno o più blocchi precedenti per prendere le fee dai miner che hanno originariamente creato

quei blocchi. Anche se ri-minare un blocco precedente ha meno probabilità di successo che estendere semplicemente la catena con un nuovo blocco, può essere più redditizio se il blocco precedente vale molto di più in fee di transazione rispetto alle transazioni attualmente nella mempool del miner.

Lo sniping delle fee è un problema che può verificarsi man mano che il Block Subsidy continua a diminuire e le fee di transazione iniziano a dominare le ricompense di blocco di Bitcoin. Se le fee di transazione sono tutto ciò che conta, allora un miner con l'x per cento del tasso di hash ha l'x per cento di possibilità di estrarre il prossimo blocco, quindi il valore atteso per loro di estrarre onestamente è l'x per cento della migliore serie di transazioni feerate nella loro mempool.

In alternativa, un miner potrebbe disonestamente tentare di ri-minare il blocco precedente più un blocco completamente nuovo per estendere la catena. Questo comportamento è indicato come fee sniping, e la probabilità del miner disonesto di avere successo se ogni altro miner è onesto è (x/(1-x))^2. Anche se il fee sniping ha una probabilità di successo complessivamente più bassa del mining onesto, tentare il mining disonesto potrebbe essere la scelta più redditizia se le transazioni nel blocco precedente hanno pagato feerate significativamente più alte delle transazioni attualmente nel mempool - una piccola possibilità per un grande importo può valere più di una grande possibilità per un piccolo importo.

Il problema è in realtà peggiore di quello descritto sopra perché ogni miner che sceglie di minare in modo disonesto riduce il numero di miner onesti che cercano di estendere la catena. Più piccola è la quota di hash rate controllata dai miner onesti, maggiore è la probabilità che un miner disonesto abbia successo, quindi un singolo grande miner che sceglie razionalmente di estrarre in modo disonesto può innescare una cascata di miner sempre più piccoli che disertano razionalmente il mining disonesto

feerate

Livello: base

Argomento: tecnologia

Feerate è il rapporto del valore delle fee, e pò riferirsi a:

- transazioni on-chain
- transazioni su Lightning Network

Nel caso delle transazioni on-chain, feerate è il rapporto che stabilisce il valore delle fee in base alla dimensione della transazione, ovvero il numero di satoshi per la dimensione della transazione in vbyte.

È utilizzato in parametri come minRelayTxFee, che specifica un feerate che funge da limite inferiore per la mempool di un nodo.

Nel caso di Lightning Network il fee_rate è una percentuale del pagamento che

viene inoltrato, generalmente misurata in ppm, parti per milione. Ha lo scopo di compensare il capitale impegnato nei canali Lightning.

Fiat

Moneta legale o a corso forzoso

Livello: base

Argomento: politica

Il termine fiat, utilizzato sia in forma autonoma che associato all'espressione fiat money, moneta fiat, è impiegato per delineare una netta separazione tra i due universi delle criptovalute e delle valute tradizionali.

Le valute tradizionali, quali il Dollaro Americano (USD), l'Euro (EUR), lo Yen (JPY), il Peso argentino (ARS), lo Zimdollar dello Zimbabwe (RTGS) e altre emesse dalle banche centrali o dagli stati, sono comunemente definite come valute "fiat". Tale definizione sottolinea il fatto che queste valute sono emesse e garantite da un'autorità sovrana, come un governo centrale o una banca centrale.

L'etimologia della parola fiat deriva dal latino e significa "sia fatto", enfatizzando il concetto che la moneta fiat acquisisce valore non in virtù di alcun supporto intrinseco, ma piuttosto attraverso l'approvazione e il riconoscimento dell'autorità sovrana. Questa distinzione è particolarmente rilevante nel confronto con le criptovalute, come il Bitcoin, le quali si basano su tecnologie di crittografia e reti peer-to-peer per garantire la sicurezza e la validità delle transazioni senza l'intervento di un'autorità centrale.

La moneta fiat rappresenta un mezzo di scambio legale, basato sulla fiducia e sulla dichiarazione dell'ente emittente e dai governi associati che la impongono e quindi viene passivamente accettata come forma di pagamento all'interno del proprio territorio.
Vengono a questo proposito anche chiamate "valute a corso forzoso" proprio perché il loro uso è imposto con la forza.
Questo aspetto è di fondamentale importanza per creare la fiducia necessaria per consentire le transazioni economiche quotidiane con questo mezzo. A differenza delle criptovalute come il Bitcoin, che operano su una rete decentralizzata e sono svincolate da qualsiasi autorità centrale, le valute fiat sono direttamente influenzate dalla politica monetaria, dalle decisioni governative e dai meccanismi di controllo economico attuati dal governo emittente.

In sintesi, il termine "fiat money" o "moneta fiat" rappresenta la modalità di imposizione dello strumento utilizzato nell'economia tradizionale, sottolineando l'importanza dell'autorità sovrana e delle politiche economiche nel conferire valore alle valute nazionali. Tale concetto trova un contrappeso nel mondo delle criptovalute con il Bitcoin, grazie alle sue caratteristiche quali decentralizzazione, sull'immunità da interferenze esterne, incensurabilità e sulla trasparenza offerta dalla tecnologia blockchain.

Fibonacci Retracement

Ritracciamento di Fibonacci

Livello: avanzato

Argomento: finanza

Il metodo di ritracciamento di Fibonacci utilizza una serie di numeri chiave chiamati rapporti di Fibonacci per identificare i livelli di supporto e resistenza di un asset/azione/criptovaluta. Viene effettuato disegnando nel grafico dell'andamento delle linee orizzontali che rappresentano i livelli di ritracciamento di Fibonacci che rappresentano i livelli di supporto e resistenza. Ogni livello corrisponde a un determinato rapporto o percentuale. Illustra fino a che punto il prezzo ha cercato di invertire un movimento precedente. Si prevede che la tendenza precedente continuerà allo stesso modo. Tuttavia, prima che ciò accada, il prezzo normalmente ripercorre uno dei suddetti rapporti.

FIBRE

Acronimo di: Fast Internet Bitcoin Relay Engine

Livello: avanzato

Argomento: tecnologia

La Relay Network Bitcoin originale è stata sostituita nel 2016 con l'introduzione del Fast Internet Bitcoin Relay Engine o FIBRE, anch'esso creato dallo sviluppatore principale Matt Corallo. FIBER è una Relay Network basata su UDP che inoltra i blocchi all'interno di una rete di nodi. FIBER implementa l'ottimizzazione dei blocchi compatti per ridurre ulteriormente la quantità di dati trasmessi e la latenza della rete.

Le Relay Network non sostituiscono la rete P2P di bitcoin. Si tratta invece di reti overlay che forniscono connettività aggiuntiva tra nodi con esigenze specializzate. Poiché le autostrade non sostituiscono le strade rurali, ma piuttosto scorciatoie tra due punti con traffico intenso, sono comunque necessarie piccole strade per collegarsi alle autostrade.

I blocchi sulla rete Bitcoin vengono effettivamente trasmessi in diversi pacchetti IP. Sfortunatamente, la perdita di pacchetti è un collo di bottiglia significativo per la velocità di propagazione; anche su relay network. Sebbene non accada necessariamente molto spesso, la perdita di pacchetti può causare picchi nel tempo di trasmissione, poiché i nodi devono ricomunicare i dati.

FIBER essendo basata sullo UDP, gli consente di utilizzare un trucco ingegnoso noto come Forward Error Correction (FEC). Ciò consente ai nodi di ricostruire tutti i dati trasmessi anche se alcuni di essi si sono persi durante il percorso.

FIBER è specificamente progettata per i blocchi compatti, la combinazione di FIBER con i Compact Block rendono FIBER molto veloce.

Infine, FIBER è progettata per essere un'alternativa più decentralizzata ad altre relay network. In particolare, come caratteristica chiave di FIBRE, è progettato come una sorta di "add-on" per Bitcoin Core, quindi chiunque gestisca un nodo dovrebbe essere in grado di configurare la propria rete.

FinCEN

Acronimo di: Financial Crimes Enforcement Network

Livello: intermedio

Argomento: politica

Il FinCEN è un ufficio federale di regolamentazione del Dipartimento del Tesoro degli Stati Uniti che raccoglie e analizza le informazioni sulle transazioni finanziarie al fine di combattere il riciclaggio di denaro nazionale e internazionale, il finanziamento del terrorismo e altri crimini finanziari. FinCEN è la Financial Intelligence Unit (FIU) degli Stati Uniti ed è una delle oltre 100 FIU internazionali che compongono il Gruppo Egmont, un'entità che si concentra sulla cooperazione e la condivisione delle informazioni tra le FIU. Come FIU, FinCEN è tenuta a divulgare informazioni finanziarie riguardanti sospetti proventi del crimine e potenziali finanziamenti al terrorismo.

FinCEN ottiene i dati delle transazioni e li traduce per scopi di applicazione della legge in modo che le autorità possano avere intuizioni utilizzabili. È responsabile del monitoraggio di comportamenti finanziari sospetti e della deterrenza del crimine finanziario. FinCEN coordina con i regolatori federali e le FIU per segnalare, analizzare e servire come controllore sui sistemi economici globali. L'obiettivo è quello di raggiungere la cooperazione con le controparti nazionali e internazionali per combattere il riciclaggio di denaro nazionale e internazionale, il finanziamento del terrorismo e altri crimini finanziari.

È stato istituito nel 1990 dal Dipartimento del Tesoro degli Stati Uniti. La missione di FinCEN è quella di migliorare la sicurezza nazionale degli Stati Uniti, scoraggiare e rilevare attività criminali, e salvaguardare i sistemi finanziari dagli abusi, promuovendo la trasparenza nei sistemi finanziari statunitensi e internazionali.

La sua missione è quella di salvaguardare il sistema finanziario statunitense dal riciclaggio di denaro. Ha il compito di raccogliere, analizzare e diffondere i dati delle transazioni finanziarie a scopo di applicazione della legge e di costruire una cooperazione globale con organizzazioni omologhe in altri paesi e con organismi internazionali come la Financial Action Task Force (FATF).

Il FinCEN svolge i suoi compiti di regolamentazione sotto il Currency and Financial Transactions Reporting Act del 1970, il cui quadro legislativo è comunemente chiamato BSA, Bank Secrecy Act. Il BSA autorizza il Segretario del Tesoro degli Stati Uniti a emettere regolamenti finanziari per le banche e altre istituzioni finanziarie per stabilire programmi antiriciclaggio (AML) e presentare

rapporti per aiutare nelle indagini e nei procedimenti penali, fiscali e normativi, così come in alcune questioni di intelligence e antiterrorismo. FinCEN è responsabile dell'applicazione, dell'implementazione e del rispetto di questi regolamenti a livello federale, statale, locale e internazionale.

FINMA

Acronimo di: Financial Market Supervisory Authority

Autorità federale Svizzera di vigilanza sui mercati finanziari

Livello: intermedio

Argomento: politica

La FINMA è l'autorità federale indipendente di vigilanza sui mercati finanziari in Svizzera. Il suo mandato consiste nella vigilanza su banche, assicurazioni, borse, commercianti di valori mobiliari, investimenti collettivi di capitale nonché sui loro asset manager e sulle relative direzioni dei fondi. Regolamenta anche l'attività di distributori e intermediari assicurativi. La FINMA si adopera al fine di conseguire la tutela di creditori, investitori e assicurati, nonché per la salvaguardia del buon funzionamento dei mercati finanziari.

La FINMA è stata una delle prime autorità di regolamentazione ad attivarsi sui crypto asset.

La FINMA divide i token in tre categorie caso per caso:

- payment
- utility
- asset token

e li regola di conseguenza.

La FINMA ha applicato la legge sul riciclaggio di denaro ai VASP e l'ha chiarita nell'ambito dell'ultimo aggiornamento della legislazione FINMA-AMLO (articolo 10). Inoltre, ha pubblicato una guida che copre la Travel Rule il 26 agosto 2019, che è entrata in vigore il 1° gennaio 2020.

FINRA

Acronimo di: Financial Industry Regulatory Authority

Livello: intermedio

Argomento: politica

La Financial Industry Regulatory Authority (FINRA) è una società americana privata che agisce come SRO, self-regulatory organization, un'organizzazione di autoregolamentazione che regola le società di intermediazione membri e i mercati dei cambi.

FINRA è il successore della NASD, National Association of Securities Dealers, Inc.), nonché delle operazioni di regolamentazione, applicazione e arbitrato dei membri della Borsa di New York.

L'agenzia governativa degli Stati Uniti che funge da regolatore finale del settore dei titoli statunitensi, inclusa la FINRA, è la SEC (US Securities and Exchange Commission).

FinTech

Livello: base

Argomento: finanza

Non esiste una definizione universalmente applicabile del termine FinTech. È una combinazione delle parole "financial services" (servizi finanziari) e "technology" (tecnologia) e si riferisce a società che offrono servizi finanziari specializzati e particolarmente orientati al cliente con l'aiuto della tecnologia moderna, cercando di migliorare e automatizzare l'adozione e l'uso dei servizi finanziari.

Il FinTech è un settore emergente che migliora la struttura esistente dei servizi finanziari convenzionali sfruttando i nuovi sviluppi tecnologici. Generalmente, mira a ridurre i costi, migliorare i tempi di transazione, rimuovere le soglie minime, rafforzare l'inclusione finanziaria e offrire termini più flessibili sui prodotti finanziari, tra le altre iniziative. Blockchain e criptovalute possono essere considerate una categoria all'interno della sfera FinTech.

Quando il FinTech è emerso nel 21° secolo, il termine è stato inizialmente applicato alla tecnologia impiegata nei sistemi di back-end delle istituzioni finanziarie consolidate. Da allora, tuttavia, c'è stato uno spostamento verso servizi più orientati al consumatore, portando a una definizione più incentrata sul cliente.

FinTech ora include diversi settori e industrie come l'istruzione, i servizi bancari al dettaglio, la raccolta fondi e il non profit, e la gestione degli investimenti, per citarne alcuni. FinTech comprende anche lo sviluppo e l'utilizzo di criptovalute come Bitcoin.

Fixed supply

Livello: base

Argomento: economia

Fixed supply, o offerta fissa, significa che la supply, o la quantità totale di un asset, è costante e non cambia.

Quando un asset ha un'offerta fissa - come ad esempio l'offerta fissa di 21 milioni di bitcoin - il fattore principale che influisce sulle fluttuazioni del prezzo è la domanda. L'offerta di un asset è correlata all'elasticità del prezzo di un asset,

ovvero alla reattività della quantità di beni o servizi necessari per modificarne il prezzo.

Quando un asset ha un'offerta fissa, l'elasticità di un asset è detta pari a zero.

Flash crash

Livello: intermedio

Argomento: finanza

i flash crash sono dovuti in linea di massima alla manipolazione, da parte delle whale che improvvisamente iniziano ad effettuare vendite in modo massiccio, in questo modo consolidano i profitti, spingono in basso le quotazioni, alimentando il panico nei piccoli investitori e potendo quindi ricomprare a un prezzo inferiore, aumentando ulteriormente le loro scorte. Man mano che scattano gli stop loss dei trader, quindi, il prezzo scivola ancora in più basso, il panico dilaga sul mercato e le balene si fiondano a comprare il nuovo fondo; questi fenomeni su bitcoin stanno iniziando a diventare sempre più rari a causa dell'elevata liquidità, ma sulle altcoin, che spesso hanno bassi volumi, sono ancora molto frequenti.

Flash dump

Livello: intermedio

Argomento: finanza

I Flash dump sono vendite effettuate in modo massiccio da parte degli speculatori, tipicamente whale, con l'intendo di provocare dei flash crash

Flash loan

Livello: avanzato

Argomento: tecnologia

Un flash loan è un prestito di criptovaluta che viene erogato e rimborsato istantaneamente. Ciò significa che un prestito di criptovaluta può essere preso in prestito e rimborsato in meno di un minuto. È un tipo di prestito DeFi che viene eseguito rapidamente - preso in prestito e restituito in rapida successione - senza la necessità di garanzie, reso possibili grazie al modo in cui i dati sono registrati sulla blockchain di Ethereum. Se il capitale e gli interessi non vengono rimborsati entro una transazione Ethereum, il flash loan viene revocato.

Non c'è alcun ritardo tra il prestito e la restituzione dei fondi poiché tutto viene gestito in modo sincrono. La componibilità atomica è quindi necessaria per il funzionamento dei flash loan, in quanto tutto deve risolversi o fallire allo stesso tempo. I flash loan non richiedono garanzie perché non c'è rischio di credito o di controparte. Di conseguenza, i flash loan sono estremamente efficienti dal punto di vista del capitale, poiché offrono un'elevata quantità di leva finanziaria.

Questo tipo di efficienza del capitale è raggiungibile solo nella DeFi e non nei mercati finanziari regolari. I flash loan sono spesso finanziati attraverso protocolli di prestito, come Aave o CREAM, che forniscono prestiti a transazione singola come funzione che permette di combinarli con altre dApp, come Uniswap o Sushiswap. Anche se le transazioni sono rapide, i flash loan non sono al sicuro dagli exploit, di solito si usa il termine flash loan attack per indicare tipo di attacco DeFi in cui un attore ostile ottiene un flash loan attraverso un lending protocol e manipola il mercato a suo favore utilizzando diversi tipi di tecniche black-hat. Le forme più popolari di attacchi DeFi sono gli attacchi flash loan, che sono i più economici da realizzare e i più semplici da portare a termine. Con un flash loan, un utente può prendere in prestito quanto vuole senza alcun costo iniziale. Ad esempio si possono prendere in prestito 50.000 dollari in ETH, per esempio, un lending protocol te li fornirà istantaneamente, ma questo non implica che siano tuoi. Devi fare qualcosa con i fondi presi in prestito per ripagare il debito e forse intascare i fondi rimanenti. Perché questo funzioni, la procedura deve essere veloce, e il debito deve essere pagato al protocollo prontamente, altrimenti la transazione sarà annullata. Poiché l'impegno a pagare il prestito è imposto da una blockchain, un prestatore decentralizzato non richiede garanzie da voi. Gli attaccanti dei flash loan si basano sull'ideazione di nuovi modi per distorcere il mercato, pur aderendo alle leggi della blockchain.

Alcuni esempi popolari di attacchi di flash loan sono l'attacco di PancakeBunny, l'hack del protocollo Alpha Homora, l'attacco di flash loan dell'aggregatore DeFi yield farming ApeRocket e molti altri. Per evitare tali attacchi, invece di dipendere da un singolo DEX per la sua alimentazione dei prezzi, le piattaforme DeFi potrebbero sfruttare oracoli di prezzi decentralizzati come Chainklink e Band Protocol per diminuire il vettore di attacco per gli attacchi di flash loan. Il ritardo nei tempi di reazione da parte dei creatori di piattaforme DeFi è uno degli aspetti più importanti che permettono agli sfruttatori di farla franca con gli assalti ai flash loan. Per evitare che questo accada, si dovrebbero usare strumenti automatizzati. OpenZeppelin Defender, una tecnologia che permette ai project manager di identificare le vulnerabilità dei contratti intelligenti e altri comportamenti strani, permettendo loro di rispondere rapidamente e neutralizzare le minacce.

Flip

Livello: intermedio

Argomento: finanza

Flip, o Flipping, è un termine generico per indicare l'acquisto di oggetti a prezzi bassi e la loro vendita rapida per un profitto. È un termine usato per figurine da collezione, giochi e fumetti per profitto, ed è un termine diventato molto popolare nel settore degli NFT.

Flippening

Livello: intermedio

Argomento: politica

Il flippening è un evento che si verifica quando una criptovaluta supera un'altra in termini di valore di mercato o di diffusione. In altre parole, il flippening si verifica quando una criptovaluta diventa più popolare o più valutata di un'altra.

Per esempio, il flippening potrebbe verificarsi se la capitalizzazione di mercato di una criptovaluta supera quella di un'altra, oppure se il numero di transazioni o il volume di scambi di una criptovaluta supera quelli di un'altra.

Il termine "flippening" viene spesso usato per riferirsi al potenziale superamento di Bitcoin da parte di altre criptovalute, come Ethereum.

Tuttavia, il termine flippening può riferirsi a qualsiasi situazione in cui una criptovaluta diventa dominante rispetto ad un'altra.

FOK

Acronimo di: Fill Or Kill Order

Livello: avanzato

Argomento: finanza

Alcuni exchange e piattaforme di trading offrono un tipo di ordine noto come "Fill or Kill Order" (FOK). Il termine si riferisce all'idea che l'ordine deve essere eseguito immediatamente nella sua interezza o non essere eseguito affatto. È strettamente legato al tipo di ordine "Tutto o niente", che si riferisce a un ordine che deve essere eseguito nella sua interezza o per niente. Gli ordini Fill or Kill sono spesso utilizzati quando un trader non vuole accettare una consegna parziale. Per esempio, quando hanno una richiesta basata sul tempo per riempire i loro ordini su mercati o scambi distinti e non collegati. Quindi un ordine FOK permetterebbe di creare più ordini e aspettare che uno venga eseguito completamente senza correre il rischio di ricevere riempimenti parziali. Dopo che uno degli ordini viene eseguito per intero, il trader è in grado di cancellare gli altri.

Un esempio di un caso d'uso Fill or Kill potrebbe essere il seguente scenario: Alice vuole impostare immediatamente un masternode di altcoin, ma uno dei requisiti per eseguire un masternode è che deve possedere 1000 unità di quella particolare criptovaluta. Se il tempo non fosse un fattore limitante, Alice potrebbe piazzare numerosi ordini di acquisto fino a raggiungere la soglia delle 1000 unità. Tuttavia, poiché vuole che il masternode sia attivo e funzionante senza troppi ritardi, può piazzare più ordini di acquisto Fill o Kill per 1000 unità dell'altcoin (in diverse borse). In questo modo, Alice pagherà gli altcoin solo se otterrà le 1000 unità che vuole e questo le permette di annullare qualsiasi ordine che non viene riempito nella sua interezza.

FOMC

Acronimo di: Federal Open Market Committee

Comitato federale del mercato aperto

Livello: avanzato

Argomento: politica

Il FOMC è un comitato all'interno del Federal Reserve statunitense, incaricato dalla legge degli Stati Uniti di supervisionare le operazioni di mercato aperto della nazione (ad esempio, l'acquisto e la vendita da parte della Fed di titoli del Tesoro degli Stati Uniti). Questo comitato prende decisioni chiave sui tassi di interesse e sulla crescita dell'offerta di moneta degli Stati Uniti. Secondo i termini dell'originale Federal Reserve Act, ciascuna delle banche della Federal Reserve era autorizzata ad acquistare e vendere nel mercato aperto obbligazioni e obbligazioni a breve termine del governo degli Stati Uniti, accettazioni bancarie, trasferimenti.

FOMO

Acronimo di: Fear Of Missing Out

Paura di essere tagliati fuori

Livello: intermedio

Argomento: finanza

La traduzione più diffusa di FOMO, fear of missing out, in italiano è "paura di essere tagliati fuori". Questa espressione coglie bene il significato del termine inglese, che indica l'ansia di perdere esperienze o eventi piacevoli che stanno vivendo gli altri.

Altre possibili traduzioni, meno utilizzate ma comunque valide, includono: * paura di rimanere indietro * ansia da esclusione * sindrome da perditore

Tutte queste traduzioni enfatizzano l'aspetto negativo della FOMO, ovvero la sensazione di inadeguatezza e di frustrazione che deriva dal sentirsi esclusi.

È la paura di perdere un' occasione che potrebbe sfuggire: nel contesto degli investimenti si riferisce al sentimento di apprensione che deriva dal poter perdere un'opportunità di investimento potenzialmente redditizia.

Tale paura viene sfruttata creando delle offerte limitate in quantità, con dei tempi di scadenza e dinamiche sul prezzo tali da spingere potenziali interessati ad aderire il prima possibile.

Le decisioni prese in questo stato spesso si rivelano avventate.

force close

chiusura forzata

Livello: intermedio

Argomento: tecnologia

Una force close di un canale Lightning Network è la chiusura unilaterale di un canale da parte di uno dei partecipanti, senza il consenso dell'altro.

Normalmente i canali vengono chiusi in modo collaborativo tra i partner del canale tramite una closing transaction firmata da entrambi i partner.

Tuttavia, ognuno dei partner potrebbe non essere disponibile o per altre ragioni non essere in grado o non voler firmare la propria transazione di chiusura. In questo caso, la parte che intende chiudere il canale può effettuare in qualsiasi momento una force close trasmettendo una commitment transaction alla rete Bitcoin.

A seguito della trasmissione della commitment transaction e la sua conferma in blockchain, vengono creati due output spendibili - uno per ciascun partner.
Il partner che ha avviato la chiusura forzata ha il proprio output con un time-lock che impedisce di essere speso subito, mentre l'output dell'altro partner è immediatamente spendibile.
Questa configurazione protegge da un comportamento fraudolento.

La force close avviene spesso in modo legittimo per motivi validi, ad esempio se il nodo di un partner diventa irraggiungibile, l'altro pubblica l'ultima commitment transaction.

Ma la force close può avvenire anche in modo fraudolento inviando alla rete una versione più vecchia, e quindi obsoleta, della transazione.
La rete non è in grado di distinguere se la transazione trasmessa sia la più recente o una più vecchia, e quindi il time-lock che impedisce per un tempo specificato a chi l'ha trasmessa di spendere i relativi output della transazione per un determinato tempo, consente all'altro partner, nel caso la transazione sia obsoleta, di avere tempo per pubblicare una Justice Transaction utilizzando il secret di revoca, che gli permette di punire il comportamento scorretto rivendicando tutti i fondi del canale per sé: la transazione di force close viene revocata (Revoked Lightning Force Close) con penalità (Force closed with penalty).

Fork

Livello: base

Argomento: tecnologia

Il termine fork letteralmente traducibile con biforcazione, indica un aggiornamento o una modifica che può essere usato sia in contesti relativi alle criptovalute e alle loro blockchain, o in altri contesti quali il software.

In relazione alla blockchain, un fork può essere definito in diversi modi, come:

- cun evento in cui una blockchain si divide in due percorsi diversi,
- una modifica al protocollo,
- o una situazione che si verifica quando due o più blocchi hanno la stessa altezza di blocco.

E può essere classificato come:

- Hard fork: un cambiamento al sistema che non è retrocompatibile. Tutti i nodi ed eventualmente i wallet devono aggiornarsi alle nuove regole per continuare a funzionare correttamente;
- Soft fork: un cambiamento al sistema che è retrocompatibile finché la maggioranza dei miner lo applica. I full node che non si aggiornano potrebbero non essere in grado di verificare i blocchi generati dopo il fork, il che potrebbe portare a una riduzione della sicurezza.
- Chain fork o Chain split: un evento in cui due o più blocchi hanno lo stesso numero di blocco, o altezza del blocco, sulla blockchain. Questo può accadere quando due miner minano quasi in contemporanea lo stesso blocco, è un evento previsto e tipicamente alcune volte alla settimana per caso e viene risolto con i nodi che si allineano alla catena più lunga, ma in casi particolari potrebbe essere causato da problemi più gravi.

I fork nella blockchain sono causati dal fatto che i diversi partecipanti devono utilizzare regole comuni per mantenere la cronologia della blockchain.

Quando i partecipanti non sono d'accordo sulle regole, possono emergere catene alternative.
Mentre la maggior parte dei fork è temporanea, alcuni sono permanenti.
I fork temporanei sono causati dalla difficoltà di raggiungere un rapido consenso in un sistema distribuito, ad esempio quando più miner generano un nuovo blocco a distanza di tempo molto ravvicinata.
I fork permanenti, che possono essere modifiche al protocollo, posso essere effettuati per aggiungere nuove funzionalità a una blockchain, possono anche essere usati per invertire gli effetti dell'hacking come nel caso di Ethereum ed Ethereum Classic, o per evitare bug catastrofici su una blockchain come nel caso del fork bitcoin del 6 agosto 2010.

Il termine fork nasce e viene usato anche per contesti diversi dalla blockchain:

- **Software fork**: creare un nuovo progetto partendo dal codice di un progetto open source esistente.
- **fork di un repository su git**: è un modo per contribuire a un progetto senza apportare modifiche al repository originale. Se si vuole contribuire a un progetto ma non si può o si vuole apportare modifiche al repository originale, è possibile creare un fork e quindi creare una pull request per le modifiche. Se la pull request viene accettata, le modifiche verranno incorporate nel repository originale.

FOSS

Acronimo di: Free and Open Source Software

Livello: intermedio

Argomento: legale

Quando si parla di software open source, OSS, a volte viene utilizzato il termine FOSS che aggiunge la parola Free ad OSS, indicando che non solo di quel software può essere visto e consultato il sorgente, ma che tale sorgente è Free. Nel contesto del software open source, la parola "free" può assumere diversi significati in italiano:

- Gratuito: uno dei significati più comuni di "free" è "gratuito". Nel contesto del software open source, questo significa che il software può essere scaricato, utilizzato, modificato e distribuito senza pagare alcun costo.
- Libero: un altro significato comune di "free" è "libero", che si riferisce alla libertà degli utenti di eseguire, studiare, condividere e modificare il software. Nel contesto del software open source, questo significa che gli utenti hanno il controllo completo del software e possono utilizzarlo come meglio credono, a patto di rispettare i termini della licenza.
- Indipendente: è il termine "free" utilizzato in Free and Open-Source Software (FOSS), per definire l'indipendenza di software. in questo caso si fa riferimento al fatto che il software è libero dal controllo di entità esterne, e quindi può essere utilizzato, modificato e distribuito in modo indipendente.

"Free" può assumere anche il significato di "libero da" per esempio, software libero da malware, libero da spyware, libero da pubblicità, o da ogni altro tipo di restrizione per quanto riguarda l'utilizzo, il distribuzione, e la modifica.

In generale, l'uso della parola "free" nel software open source si riferisce alla combinazione di gratuità e libertà, e all'indipendenza del software, che permette agli utenti di utilizzare, modificare e distribuire il software senza restrizioni e senza dover pagare alcun costo.

I software open source (OSS) e i software liberi (FOSS) sono quindi simili ma ci sono alcune differenze tra i due:

- Il software open source OSS è caratterizzato dal fatto che il codice sorgente è disponibile per chiunque e può essere modificato e distribuito a proprio piacimento. Ciò significa che gli utenti possono esaminare il codice sorgente, apportare modifiche e personalizzare il software in base alle proprie esigenze. In generale, il software open source è creato da una comunità di sviluppatori che lavorano insieme per migliorare il software.
- Il software libero FOSS, è simile al software open source, ma c'è una forte enfasi sulla libertà degli utenti di utilizzare, modificare e distribuire il software. Ciò significa che gli utenti possono utilizzare il software per qualsiasi scopo senza restrizioni, e che possono contribuire al miglioramento del

software attraverso la modifica del codice sorgente.

In sintesi le differenze sono: * OSS si concentra principalmente sulla disponibilità del codice sorgente, e sulla possibilità di modificarlo e distribuirlo. * FOSS si concentra sulla libertà degli utenti di utilizzare, modificare e distribuire il software. * In generale entrambi i tipi di software sono gratuiti e spesso i termini OSS e FOSS vengono usati come sinonimi.

Esiste una ulteriore specifica del software OSS e FOSS, che è il software Reproducible, o Riproducibile, che garantisce all'utente non solo di vedere il sorgente e distribuirlo, ma di creare dal sorgente il programma in autonomia.

FPGA

Acronimo di: Field Programmable Gate Array

Livello: intermedio

Argomento: tecnologia

Un FPGA (Field-Programmable Gate Array) è un tipo di dispositivo hardware programmabile che può essere configurato per svolgere diverse funzioni attraverso la programmazione del suo circuito logico.
Nei primi anni del mining di Bitcoin, l'uso di FPGA è stato introdotto come un'alternativa più efficiente rispetto all'utilizzo di CPU e GPU.

L'apparizione del mining con GPU nel 2010 e l'impennata del prezzo del BTC hanno infatti portato a una corsa nel settore del mining, e i miner cercavano costantemente nuovi modi per migliorare le loro capacità di calcolo.

Poiché gli FPGA possono essere configurati per eseguire in parallelo operazioni specifiche, possono raggiungere velocità di hashing più elevate rispetto alle CPU e alle GPU general-purpose.

Nel 2011, qualcuno ha condiviso il codice delle macchine di mining FPGA su GitHub, dando inizio a una nuova era dominata da sistemi di mining specializzati. Nel 2011, l'hash rate Bitcoin è salito da 116 GH/s all'inizio dell'anno a quasi 30 TH/s alla fine dell'anno, una crescita di quasi 300 volte.

I miner di Bitcoin utilizzavano i FPGA per creare macchine di mining personalizzate, programmando gli FPGA con l'algoritmo di hashing Bitcoin per aumentare la velocità di calcolo e ottenere una maggiore potenza di hashing. Questo ha permesso loro di generare un maggior numero di tentativi per trovare nuovi blocchi di transazioni e guadagnare le ricompense in Bitcoin.

Nel 2012 è nato il mining con macchine ASIC ancora più specializzate nel mining di Bitcoin, gli FPGA sono stati progressivamente sostituiti come opzione preferita per il mining, poiché gli ASIC offrivano prestazioni ancora superiori in termini di velocità di hashing e consumo energetico ottimizzato, e il tasso di hash di Bitcoin è schizzato da 20 TH/s a 12 PH/s, un aumento di 600 volte. Da

allora, i modelli ASIC hanno sostituito le CPU, le GPU e le macchine FPGA come macchine per il mining Bitcoin.

FPPS

Acronimo di: Full Pay Per Share

Livello: avanzato

Argomento: tecnologia

FPPS è un tipo di pagamento dei miner che partecipano ad una mining pool, tramite il quale sia la ricompensa del blocco che il costo del servizio di mining sono regolati in base al profitto teorico.

Viene calcolata una commissione di transazione standard entro un certo periodo e la distribuisce ai miner in base ai loro contributi di potenza hash nel pool. Aumenta i guadagni dei miner condividendo una parte delle commissioni di transazione.

Con i metodi di pagamento PPS e FPPS, si viene pagati indipendentemente dal fatto che il pool trovi o meno un blocco. Questo è il vantaggio più significativo rispetto a PPLNS. I rischi e le ricompense sono maggiori con il piano PPLNS.

Front running

Livello: avanzato

Argomento: finanza

Il Front running è una manipolazione del mercato in cui un bot può concludere una transazione prima di un ordine in sospeso (o in arrivo) impattando sul prezzo dell'ordine stesso.
Questa attività viene effettuata tramite bot su piattaforme DeFi.

I bot possono eseguire la scansione degli ordini in sospeso e possono inserire prima le loro operazioni, approfittando così dei movimenti di prezzo risultanti quando gli ordini precedenti vengono infine eseguiti.
I bot intercettano gli ordini prima che vengano confermati e si adeguano di conseguenza in base a quello che sta per succedere.
Se questi ordini sono di importo elevato, possono avere un impatto sul prezzo dell'asset. I bot acquistano grosse quantità di quel token (se ci sono grossi ordini di buy) o lo vendono (in caso contrario). In tal modo, essi traggono profitto dall'aumento del prezzo o evitano di subire perdite per la diminuzione dello stesso (nel caso di vendita). Il front-running è connesso allo slippage.

Il front-running su Ethereum avviene facilmente perché i bot sono in grado di offrire un gas fee leggermente più alto su una transazione, incentivando i miner a piazzare prima il loro ordine durante la convalida del blocco.
Le transazioni più remunerative vengono inserite nel blocco per prime dai miner.

FROST

Acronimo di: Flexible Round-Optimized Schnorr Threshold

Soglia di Schnorr Ottimizzata per Round Flessibili

Livello: avanzato

Argomento: tecnologia

FROST è l'acronimo di "Flexible Round-Optimized Schnorr Threshold" (Soglia di Schnorr Ottimizzata per Round Flessibili).

Si basa sulle firme di Schnorr, introdotte nel 2019 su Bitcoin, e gli indirizzi Taproot di Bitcoin, attivi dal 2021, due tra gli sviluppi più interessanti degli ultimi anni.

In parole semplici, FROST permette a un gruppo di utenti di creare insieme una chiave condivisa che sembra provenire da un singolo proprietario, anche se in realtà è controllata da più persone in modo collaborativo.

Questo fornisce un enorme vantaggio di privacy: infatti sulla blockchain è impossibile distinguere se un indirizzo è controllato da una singola chiave o da una chiave multi-firma.

Gli utenti generano le loro chiavi private e poi, interagendo tra loro off-chain, producono una chiave condivisa che può essere usata per spendere i bitcoin. Solo un numero minimo di firme, generate in modo casuale e univoco, è necessario per autorizzare una transazione.

Ad esempio, un gruppo di 3 amici potrebbe creare un portafoglio 2-su-3, dove solo 2 firme casuali e univoche sono necessarie per spendere i bitcoin. Ma per un osservatore esterno, quell'indirizzo sembrerà appartenere ad un singolo proprietario.

Caratteristiche principali di FROST: * **Firme multiple**: Permette a più partecipanti di generare una firma congiunta senza rivelare le loro chiavi private individuali. * **Threshold Signatures**: FROST consente la creazione di firme che richiedono la collaborazione di almeno una soglia minima di partecipanti (ad esempio, 3 su 5) per firmare una transazione. Questo è utile in contesti in cui si vuole garantire che una transazione possa essere autorizzata solo con l'approvazione di una certa maggioranza. * **Efficienza**: A differenza di altri protocolli di firma, FROST è progettato per ridurre il numero di round di comunicazione necessari tra i partecipanti, rendendolo più veloce e scalabile. * **Sicurezza**: FROST mantiene un elevato livello di sicurezza crittografica, distribuendo la responsabilità tra più parti e assicurando che un attaccante non possa generare firme valide senza la collaborazione del numero minimo richiesto di partecipanti. * **Privacy**: Le firme generate con FROST non rivelano quanti partecipanti hanno contribuito alla firma, né l'identità dei partecipanti stessi, migliorando la privacy delle transazioni.

Applicazioni:

FROST è particolarmente utile in contesti di multi-firma, dove più parti devono autorizzare una transazione Bitcoin. Ad esempio, può essere utilizzato in wallet di tipo multisig, in organizzazioni decentralizzate, o in sistemi che richiedono un alto livello di sicurezza, come le custodie di Bitcoin gestite da più individui o enti.

In sintesi, FROST è un protocollo avanzato che migliora la sicurezza, l'efficienza e la privacy delle firme digitali nel contesto di Bitcoin, utilizzando la crittografia Schnorr.

FSB

Acronimo di: Financial Stability Board

Consiglio per la stabilità finanziaria

Livello: intermedio

Argomento: politica

L'FSB, Financial Stability Board o Consiglio per la stabilità finanziaria, è un'organizzazione internazionale il cui scopo è monitorare il sistema finanziario mondiale.

L'FSB ha annunciato a Ottobre 2022 una serie completa di proposte per la regolamentazione e la supervisione delle attività di criptovalute.

FSS

Acronimo di: First-Seen-Safe

Livello: intermedio

Argomento: tecnologia

FSS o First-Seen-Safe, in italiano "Quella vista per prima è sicura", si riferisce ad un comportamento dei nodi della rete bitcoin rispetto alle nuove transazioni ricevute, che controllano se nella mempool c'è già un'altra transazione che spende lo stesso input UTXO, e nel caso in cui tale transazione venga trovata, la nuova viene rifiutata e non viene inclusa nel mempool di questo nodo e non viene propagata ulteriormente alla rete.

È una modalità di comportamento che vorrebbe limitare la possibilità di double spend.

Ma è una modalità che generalmente non viene applicata dai nodi o dai miner Bitcoin, perché i miner sono incentivati a selezionare le transazioni che hanno delle fee più alte, e le opzioni RBF e Full RBF consentono agli utenti di sostituire una transazione Bitcoin prima che venga confermata nella blockchain con una

nuova transazione spendendo nuovamente lo stesso input della transazione, solo con una commissione più alta.

Inoltre le transazioni Bitcoin vengono trasmesse attraverso un sistema distribuito asincrono in cui non esiste un "primo" a livello globale che riceve la transazione. Quello che Alice ha visto per prima, Bob potrebbe vederlo per secondo. Il design di Bitcoin non prevede un meccanismo che consenta ad Alice e Bob di accordarsi su quale transazione sia stata realmente la prima; tutto ciò che possono fare è aspettare di vedere quale di queste transazioni viene confermata in un blocco valido della migliore catena di blocchi.

FT

Acronimo di: Fungible Tokens

Token fungibili

Livello: base

Argomento: tecnologia

I token fungibili sono così chiamati perché hanno la proprietà di fungibilità, ovvero ogni token vale quanto un altro token e quindi sono rappresentabili semplicemente tramite il loro quantitativo, non hanno un identificatore univoco associato o altri dati che li differenziano. Per questa ragione sono utilizzati per rappresentare una valuta all'interno di ogni blockchain.

FUD

Acronimo di: Fear, Uncertainty, and Doubt

paura, incertezza e dubbio

Livello: base

Argomento: finanza

È spesso una strategia di marketing basata sulla diffusione di informazioni negative, vaghe e inaccurate sul prodotto di un concorrente, in modo da creare un clima di sfiducia verso la concorrenza. La strategia si estende ad altri ambiti, quali, ad esempio, la propaganda politica o l'introduzione di innovazioni tecnologiche.

Full Node

nodo completo

Livello: base

Argomento: tecnologia

I Full Node sono nodi che scaricano l'intera cronologia di una blockchain e la tengono aggiornata con i nuovi blocchi.

Un full node aiuta il funzionamento della rete peer to peer, scaricando dagli altri nodi transazioni e blocchi, effettuandone la verifica e inoltrandoli a ulteriori nodi della rete.

La maggior parte dei full node offrono i propri servizi ai lightweight client consentendo loro di trasmettere le proprie transazioni alla rete e avvisandoli quando una transazione influisce sul loro portafoglio. Se i nodi che eseguono questa funzione non sono sufficienti, i client non saranno in grado di connettersi tramite la rete peer-to-peer e dovranno invece utilizzare servizi centralizzati.

Un full node mantiene e aggiorna le seguenti informazioni:

- **chain state**: il chain state, o stato della chain, contiene le informazioni relative agli utxo, o utxo set
- **blocks db**: reppresenta il database che memorizza tutti i blocchi della block chain
- **mempool**: la mempool, l'area temporanea di transito delle transazioni non confermate attraverso la quale le transazioni vengono propagate ai nodi prima di essere inserite nella block chain

Il nodo ha comunicazioni:

- **inbound**: o in ingresso, il nodo accetta connessioni in ingresso che vengono iniziate da nodi esterni per collegarsi al nodo; un nodo può avere fino a 117 connessioni inbound

- **oubound**: o in uscita: le connessioni outbound vengono iniziate dal full node per collegarsi ai nodi esterni. Un nodo stabilisce 8 connessioni outbound

- **Banlist**: il nodo mantiene una lista di nodi ai quali proibisce di avere delle connessioni, spesso a causa di comportamenti sospetti o violazione del protocollo.

- **Whitelist**: la lista di nodi che ricevono permessi speciali

Un full node comunica con il mondo esterno attraverso i seguenti protocolli di comunicazione:

- **RPC**: Remote procedure call, è il protocollo che consente al software locale di comunicare con il full node
- **http**: il protocollo http, quello nato per il web, fornisce una interfaccia che consente agli utenti di interagire con il nodo tramite un browser web
- ZMQ: ZeroMQ è una libreria di messaggi asincroni, spesso utilizzata per avere notifiche su transazioni e blocchi

Esistono diverse implementazioni software del full node, tra questi:

- Bitcoin Core considerato l'implementazione che attualmente rappresenta lo standard de facto per Bitcoin
- Bitcoin Knots
- Libbitcoin
- nix-bitcoin
- btcd

Full RBF

Livello: intermedio

Argomento: tecnologia

Con Full RBF, si intende una impostazione di un full node che consente la Transaction Replacement, o sostituzione della transazione tramite la modifica delle fee o RBF Replace-by-fee, quando si trova ancora nella mempool, quindi non è stata ancora confermata.

Esistono due forme di RBF:

- opt-in RBF, nel quale è l'utente che segnala quando crea la transazione che vuole poter modificare le fee nel caso la transazione, e per questa sono state definite delle specifiche nel BIP 125
- Full RBF, ovvero il nodo è impostato per consentire la sostituzione della transazione quando ci siano delle condizioni opportune anche se l'utente non ha esplicitamente impostata la transazione come RBF.

Full RBF consente incondizionatamente a una transazione di sostituire quelle più vecchie, purché paghi una fee sufficiente.

Bitcoin Core consente attraverso il parametro -mempoolfullrbf di impostare la modalità Full RBF, ma di default questo parametro è impostato a off (disabilitato) anche nell'ultima versione 24.0 rilasciata a novembre 2022. Era stato proposto per la versione Bitcoin Core di impostare questo parametro come attivato di default, ma su questa decisione si è accesa una discussione sulle sue conseguenze sulla possibilità di accettare transazioni non confermate o 0-conf nel caso che l'impostazione default Full RBF si diffonda.

Da ottobre 2023 è disponibile una particolare versione di Bitcoin Core, denominata Full-RBF Peering Bitcoin Core v25.1

È la versione v25.1di Bitcoin Core, che di default ha il parametro full-rbf attivo mempoolfullrbf=1 mentre la v25.1 "normale" ha questo parametro disattivato di default, anche se che chi fa girare il nodo può decidere di attivarlo.

Questa versione fa anche qualcos'altro:

1. Quando mempoolfullrbf è =1, rende noto agli altri nodi questa impostazione con un apposito bit di servizio FULL_RBF

- Si connette a quattro peer FULL_RBF aggiuntivi.

In questo modo si vuole garantire che un gruppo principale di nodi propaghi in modo affidabile le sostituzioni full-rbf.

Funding Transaction

Livello: intermedio

Argomento: tecnologia

In Lightning Network, una Funding Transaction è una transazione che viene utilizzata per creare un canale di pagamento sulla rete Lightning. Un canale di pagamento su Lightning Network è un modo per trasmettere denaro tra due parti senza dover memorizzare tutte le transazioni on-chain. Invece, i due partecipanti al canale di pagamento mettono in comune una somma di denaro, che viene "congelata" sulla blockchain principale in modo che possa essere utilizzata solo attraverso il canale di pagamento.

La Funding Transaction viene utilizzata per inizializzare il canale di pagamento. Essa fornisce l'importo di denaro che verrà congelato e utilizzato attraverso il canale di pagamento e gli indirizzi Bitcoin dei due partecipanti. Una volta che la Funding Transaction è stata confermata sulla blockchain, il canale di pagamento può essere utilizzato per effettuare pagamenti tra i due partecipanti senza dover utilizzare la blockchain principale per ogni singola transazione. Questo rende possibile effettuare pagamenti rapidi e a basso costo sulla rete Lightning.

Due parti creano una transazione finanziata da singoli input, ad esempio Alice fornisce un UTXO da 10 bitcoin come input. Questa Funding Transaction crea una multi-firma 2-di-2 con lo script redeem

```
2 <PubKeyAlice> <PubKeyBob> 2 CHECKMULTISIG
```

Alice e Bob possono spendere questo UTXO solo con entrambe le firme. Se una delle due è maligna, i fondi sono bloccati e irredimibili. Alice vuole proteggersi dal caso in cui il malintenzionato Bob vada off-line, quindi richiede la firma di Bob su una commitment transaction, come descritto di seguito, che invia tutti i 10 bitcoin a un nuovo script di Alice. Alice memorizza questa transazione, ma non la trasmette ancora. Ora Alice firmerà la Funding Transaction, sapendo che in qualsiasi momento potrebbe trasmettere la commitment transaction iniziale con la firma di Bob. La Funding Transaction viene verificata da ogni nodo completo e confermata nella catena temporale. Ora il canale di pagamento è aperto, ha un identificativo univoco della transazione e un ID del canale. Alice e Bob possono scegliere di annunciare pubblicamente questo canale alla rete lightning e offrire di instradare i pagamenti fino alla capacità del multisig.

Fungible

Fungibile

Livello: base

Argomento: economia

I beni fungibili sono i beni intercambiabili di cui conta il valore assegnato piuttosto che l'oggetto individuale. Ad esempio le valute fiat sono fungibili: un euro vale un euro sia che si tratti di una moneta da 1 euro, che da 2 monete da 50 centesimi. La fungibilità è una qualità fondamentale dei bitcoin, per preservare la resistenza alla censura e la privacy: l'ingerenza dei governi, attività criminali e chain analisys possono portare occasionalmente alcuni bitcoin a essere riconoscibili e conseguentemente meno fungibili, ad esempio alcuni exchange si sono rifiutati di accettare monete provenienti da azioni di coinjoin.

Futures

Livello: intermedio

Argomento: finanza

Un "contratto futures" è un accordo legale standardizzato per acquistare o vendere una determinata merce o bene ad un prezzo predeterminato in un momento specifico in futuro. Questi strumenti finanziari sono spesso utilizzati sia dagli hedger che dagli speculatori come un modo per anticipare potenziali movimenti futuri dei prezzi, sia per la copertura dai rischi che per realizzare profitti. Il regolamento del contratto avviene quando raggiunge la sua data di scadenza, a quel punto chi detiene i futures è obbligato ad acquistare o vendere l'attività sottostante al prezzo concordato. Sono diversi dai contratti a termine, che possono essere personalizzati per ogni operazione e possono essere negoziati over-the-counter, invece di essere scambiati in borsa.

GAS price

Livello: intermedio

Argomento: tecnologia

È il prezzo in GAS il meccanismo di tariffazione utilizzato sulla rete Ethereum per far eseguire una transazione o un contratto sulla blockchain di Ethereum. Il funzionamento dell'Ethereum Gas Price non è differente dall'uso dei Kw usati al fine di misurare il consumo di elettricità. Ethereum ha un limite di dimensione del blocco, quindi è necessario pagare una fee per avere più probabilità di accedere subito nel blocco successivo, proprio come succede con i Bitcoin. In quest'ultimo caso, i miner danno priorità alla transazione con le commissioni più alte. Con Ethereum avviene la medesima cosa, dal momento che i miner sono liberi di scegliere di ignorare le operazioni il cui gas limite è troppo basso. Più complessi sono i comandi che vuoi eseguire, più gas (ed Ether) dovrai pagare.

Genesis block

Blocco Genesis

Livello: avanzato

Argomento: tecnologia

Il Genesis block è il primo blocco di transazioni di una blockchain, dal quale poi si collegano in catena i blocchi successivi. Viene chiamato anche blocco 0 (zero).

La data impostata nel genesis block Bitcoin è 3 gennaio 2009. Esso rappresenta l'inizio della blockchain di Bitcoin.

Alcune delle caratteristiche peculiari del genesis block di Bitcoin sono:

- Non ha un blocco precedente: il genesis block è il primo blocco della blockchain e, come tale, non ha un blocco precedente a cui fare riferimento.
- Non contiene transazioni: il genesis block contiene solo una transazione speciale, la sola transazione Coinbase, e i 50 bitcoin di ricompensa, o Block Reward, sono assegnati all'indirizzo 1A1zP non possono essere spesi.
- Contiene un messaggio incorporato: il genesis block contiene un messaggio incorporato che recita:

```
The Times 03/Jan/2009 Chancellor on brink of second bailout for
banks
```

Il genesis block di Bitcoin è stato un evento storico importante per la rete e rappresenta l'inizio della blockchain di Bitcoin. Ancora oggi, il genesis block è considerato un simbolo dell'innovazione e della rivoluzione che Bitcoin ha rappresentato nel mondo dei pagamenti digitali.

Il blocco successivo al genesis block, il blocco 1 di Bitcoin è stato estratto solo sei giorni dopo, il 9 gennaio 2009.

La data del 3 Gennaio 2009 Il genesis block non è stato creato attraverso il processo di mining utilizzato da Bitcoin, ma è stato creato manualmente da Satoshi Nakamoto.

Nonostante il timestamp nel genesis block sia il 3 Gennaio 2009, non c'è certezza che sia stato creato esattamente in quella data.

Il messaggio incorporato che fa riferimento a un articolo pubblicato su The Times il 3 gennaio 2009, in cui si parla delle difficoltà finanziarie dei banchi, dimostra però che questo blocco e conseguentemente i successivi non potevano essere stati generati prima del 3 gennaio 2009, e quindi pre-minati, essendoci un riferimento ad un articolo che non poteva essere conosciuto prima del 3 gennaio 2009.

Gossip protocol

Livello: avanzato

Argomento: tecnologia

Il protocollo Gossip è un protocollo utilizzato in alcune reti peer-to-peer per consentire ai partecipanti o nodi di comunicare tra loro e scambiarsi informazioni, quali ad esempio gli altri nodi della rete, senza doversi affidare ad un registro o ad una lista centralizzata che diventerebbe un anello debole del sistema.

L'ispirazione per la progettazione del protocollo Gossip nasce dagli studi sulla diffusione delle epidemie e dagli algoritmi che ne derivano.

Bitcoin utilizza protocollo Gossip per distribuire i valori nonce tra ciascuno dei suoi nodi di mining. Lightning Network utilizza il protocollo Gossip per consentire la scoperta dei nodi e dei canali come dettagliato nelle specifiche BOLT 7

Vantaggi

- **Scalabilità**: il protocollo Gossip è altamente scalabile. Questo perché è possibile distribuire le informazioni con un livello di prestazioni molto efficiente: i nodi distribuiscono un numero fisso di messaggi ai nodi con cui sono correlati.
- **Robustezza**: nel protocollo Gossip tutti i nodi funzionano allo stesso modo e non hanno una funzione speciale o diversa l'uno dall'altro. Pertanto, se si verifica un errore in uno o più nodi, non influirà né interromperà la funzionalità degli altri nodi della rete per la distribuzione delle informazioni. Allo stesso modo, i nodi possono entrare o uscire dalla rete senza restrizioni e senza pregiudicarne il funzionamento.
- **Tolleranza agli errori**: poiché i nodi hanno la capacità di condividere e distribuire informazioni con più nodi nella rete peer, questi protocolli hanno la capacità di funzionare correttamente. Anche in situazioni difficili dove la connettività di alcuni nodi è compromessa. Se un determinato nodo viene disconnesso per qualsiasi motivo, le informazioni verranno distribuite allo stesso modo dagli altri nodi che hanno già ricevuto il messaggio.
- **Decentralizzazione**: i protocolli di Gossip distribuiscono le informazioni in modo completamente decentralizzato e autonomo.

Svantaggi

Sebbene i protocolli Gossip offrano robustezza al sistema consentendo ai nodi di continuare a funzionare senza interruzioni in caso di guasti, è possibile che le informazioni o il messaggio distribuito siano compromessi. Ad esempio, un attaccante può introdurre nella rete un nodo difettoso, che può modificare in modo subdolo le informazioni in modo che il messaggio rimanga leggibile, ma

allo stesso tempo contenga informazioni false o errate. E anche gli altri nodi, che opereranno senza interruzioni, distribuiranno queste informazioni.

Nel caso di Lightning Network, il protocollo Gossip rappresenta una delle criticità per lo scaling dell'intero stack del protocollo Lightning. Attualmente è molto semplice e funziona in un modo abbastanza simile alla propagazione delle transazioni sulla rete Bitcoin; i nodi della rete ricevono un messaggio di gossip, verificano il messaggio in base alle regole di validità e lo trasmettono a tutti i loro peer per propagarsi ulteriormente attraverso la rete. È un semplice protocollo flood fill che presuppone che i messaggi validi alla fine si propagheranno sull'intera rete. Per questo motivo, esiste la preoccupazione di attacchi denial-of-service (spam) che possono consumare una grande quantità di risorse di elaborazione e larghezza di banda da gestire. Nel caso della main net di Bitcoin, i nodi non trasmetteranno transazioni non valide, quindi per trasmettere qualcosa che consuma la larghezza di banda e le risorse di calcolo dei nodi richiede che tu abbia effettivamente bitcoin con cui creare una transazione. Nel caso del protocollo di gossip Lightning, è necessario dimostrare di controllare un UTXO valido che finanzia un canale per trasmettere un messaggio gossip sul canale. Questo svolge la stessa funzione di protezione antispam della rete principale di Bitcoin; non puoi spammare messaggi attraverso la rete senza controllare effettivamente dei bitcoin. Ma ha un grosso problema: una totale mancanza di privacy: per pubblicizzare il tuo canale sulla rete affinché le persone possano instradare i pagamenti, devi indicare l'esatto UTXO utilizzato per finanziare quel canale e associarlo alla chiave di identità del tuo nodo Lightning.

Governance tokens

Livello: intermedio

Argomento: politica

Token che danno ai titolari poteri di voto su un protocollo blockchain. Sono utilizzati principalmente nei progetti DeFi in modo che i sistemi possano rimanere decentralizzati e nessuna parte prenda le decisioni sulla direzione futura del progetto.

GPU

Acronimo di: Graphics processing unit

Scheda grafica

Livello: base

Argomento: tecnologia

Una GPU, acronimo di "Graphics Processing Unit" (Unità di elaborazione grafica), è un tipo di processore specializzato progettato per eseguire operazioni

ad alta intensità di calcolo legate alla grafica, come la generazione di immagini 3D, l'elaborazione video e altro ancora.

Le GPU sono comunemente utilizzate nelle schede grafiche dei computer per migliorare le prestazioni visive e la resa grafica nei videogiochi, nelle applicazioni di grafica professionale e nella riproduzione di contenuti multimediali complessi.

Le GPU possono essere usate per effettuare i calcoli per il mining in modo più efficente delle CPU utilizzate inizialmente.

Nel 2010 Laszlo Hanyecz ha inizialmente ipotizzato che le GPU potessero eseguire i calcoli del mining con velocità maggiore rispetto alle CPU.

Laszlo Hanyecz è noto soprattutto per aver effettuato il primo acquisto documentato utilizzando Bitcoin come mezzo di scambio, ovvero due pizze il 22 maggio 2010 e questo evento viene ricordato con il nome di "bitcoin pizza day".

L'utente noto con lo pseudonimo ArtForz e Laszlo Hanyecz sono considerati le prime due persone ad aver fatto mining con le GPU, utilizzando un codice di mining privato.

Nel settembre 2010, ArtForz ha sviluppato un software di mining che ha sfruttato la potenza di calcolo delle GPU per estrarre Bitcoin in modo più efficiente rispetto alle CPU.

ArtForz è arrivato a detenere una percentuale elevata di potenza di calcolo della rete Bitcoin, circa il 25%.

Dopo che Hanyecz ha condiviso il suo codice di mining con le GPU con la comunità, Bitcoin ha visto un forte aumento della potenza di calcolo di 20.000 volte, passando da 6 MH/s nel gennaio 2010 a 120 GH/s nel dicembre 2010.

L'adozione del mining con le GPU e l'impennata del prezzo del BTC hanno portato a una corsa al mining, con i miner alla costante ricerca di nuovi modi per migliorare la loro potenza di calcolo. Nel 2011, qualcuno ha condiviso il codice delle macchine di mining con FPGA su GitHub, inaugurando una nuova era dominata dalle apparecchiature specializzate per il mining che ha portato al declino dell'uso delle CPU per il mining Bitcoin.

Gresham's Law

legge di Gresham

Livello: avanzato

Argomento: politica

La legge di Gresham afferma che "la moneta cattiva scaccia quella buona". In altre parole, in un'economia in cui sono in uso due valute, gli individui spenderanno la moneta cattiva, che si svaluta costantemente, e tratterranno la moneta

buona, che conserva il suo valore. Pertanto, la moneta cattiva dominerà in termini di circolazione e utilizzo nelle transazioni quotidiane, mentre la moneta buona sarà preferita per il risparmio e l'investimento a lungo termine.

Ad esempio, nel caso di Bitcoin, un individuo che detiene sia bitcoin che dollari USA preferirà spendere i dollari, poiché questi perdono costantemente valore. Se spendesse i suoi bitcoin, perderebbe il potenziale futuro aumento della loro valutazione. Questo è uno dei motivi per cui Bitcoin è cresciuto più rapidamente come riserva di valore piuttosto che come metodo di pagamento.

La legge di Gresham è più visibile quando un governo o una banca centrale stabilisce il valore del denaro attraverso leggi sul corso legale o un peg valutario. Ad esempio, nel 1965, il governo degli Stati Uniti ridusse il contenuto d'argento delle monete da mezzo dollaro dal 90% al 40%. Sia le monete d'argento al 90% che quelle al 40% avevano lo stesso valore legale. Ciò ha portato alla fusione, all'esportazione o alla rimozione dalla circolazione della maggior parte delle monete al 90%.

La legge di Gresham spiega come l'interferenza del governo nell'offerta e nella valutazione del denaro possa danneggiare un'economia. Quando Enrico VIII d'Inghilterra svilì le monete d'argento inglesi e impose un legame impreciso tra monete d'oro e d'argento, le monete d'oro più preziose furono vendute all'estero, dove il loro prezzo non era legalmente soppresso, lasciando l'Inghilterra impoverita da denaro di bassa qualità.

griefing attack

Livello: intermedio

Argomento: tecnologia

Un griefing attack si verifica quando qualcuno invia intenzionalmente spam alle transazioni su una rete, aumentandone il carico di lavoro e interrompendone le normali operazioni.

I griefing attack spesso frustrano gli altri utenti della rete, poiché è più difficile eseguire applicazioni sul sistema, senza avvantaggiare finanziariamente l'aggressore.

Il termine arriva dal mondo dei videogiochi, dove si parla di griefing quando i giocatori dei giochi multiplayer infrangono volontariamente le regole dei server o le linee guida imposte dalla community e rovinano così il divertimento agli altri giocatori o la loro possibilità di successo.
Coloro che si comportano in questo modo, provocando virtualmente dispiacere (che è poi una delle possibili traduzioni del termine inglese grief) agli altri giocatori, vengono soprannominati griefer.

Un esempio di griefing attack è quello effettuato sotto forma di block storm sulla testnet.

Gwei

Livello: intermedio

Argomento: tecnologia

Un Gwei è una frazione di ETH (Ether, vedi), precisamente un miliardesimo ETH, quindi 1 Gwei equivale a 0.000000001 o 10-9 ETH.

Halving

Livello: intermedio

Argomento: tecnologia

L'Halving, a volte chiamato anche Halvening, indica il dimezzamento del Block Subsidy, ovvero dei nuovi Bitcoin creati in ogni blocco e dati in premio ai miner per la validazione di ogni blocco.

L'Halving ha quindi impatto sia sulla Block Reward, ovvero sulla ricompensa che serve come incentivo affinché i miner facciano il lavoro di creazione e validazione dei nuovi blocchi da aggiungere alla blockchain, e conseguente sul controllo dell'emissione di nuove monete circolanti. Questo halving o dimezzamento fa in modo che l'emissione dei Bitcoin produca una Circulating supply, o disponibilità circolante con una curva di forma asintòtica, ovvero inizia con una crescita rapida che diminuisce sempre più velocemente fino ad appiattirsi.

Nel caso di Bitcoin, l'halving avviene ogni 210.000 blocchi quindi circa ogni 4 anni.
Inizialmente il premio era di 50 bitcoin per ogni blocco, i successivi halving e corrispondenti premi o Block Subsidy sono:

BTC | blocco | Data dell'halving |
:—: | | ————- |
25 | 210000 | 28 novembre 2012 |
12,5 | 420000 | 9 luglio 2016 |
6,25 | 630000 | 11 maggio 2020 |
3,125 | 840000 | 20 aprile 2024 |

Il processo di having continuerà fino a quando saranno state minate 21 milioni di monete che si prevede avverrà nel 2140.

Il meccanismo dell'halving attribuisce a Bitcoin caratteristiche di risorsa scarsamente disponibile, resistente all'inflazione.

Hard Cap

Livello: intermedio

Argomento: tecnologia

In una ICO il termine si riferisce al limite massimo del numero di token che possono essere venduti. Si riferisce alla quantità massima di fondi che il team di sviluppo è disposto a raccogliere in cambio dei propri token durante quella fase iniziale di finanziamento.

Hard Fork

Livello: intermedio

Argomento: tecnologia

Un hard fork Bitcoin è un cambiamento nel protocollo Bitcoin che che richiede che tutti i nodi si aggiornino alle nuove regole affinché il sistema continui a funzionare.

Gli hard fork Bitcoin possono essere utilizzati per apportare modifiche al protocollo, ad esempio per correggere bug o vulnerabilità.

Altri motivi, quali:

- Aumentare la dimensione dei blocchi per migliorare la scalabilità
- Aggiungere nuove funzionalità, come il supporto per i contratti intelligenti

possono essere controversi, poiché possono portare a una divisione nella comunità Bitcoin, e a uno split o divisione della block chain. Ciò è accaduto nel 2017, quando un gruppo di sviluppatori ha creato Bitcoin Cash, un fork di Bitcoin che ha aumentato la dimensione dei blocchi.

Hard money

Livello: base

Argomento: economia

Hard money si riferisce a una forma di denaro che è scarsa, limitata nella quantità e difficile da produrre.

In relazione a Bitcoin, significa che esiste un limite massimo fisso alla quantità di Bitcoin che potranno mai essere creati: circa 21 milioni, in contrasto alle valute fiat, come il dollaro statunitense o euro che sono controllate da banche centrali e governi, i quali possono creare nuova moneta a loro discrezione tramite il Quantitative Easing, politiche di stampa di denaro o interventi monetari.

Questo limite di Bitcoin è programmato nel suo protocollo e garantisce che l'offerta sia limitata nel tempo.
Il fatto che il Bitcoin sia "hard money" suggerisce che è progettato per essere una forma di valore stabile e resistente all'inflazione.

Quindi, quando ci si riferisce a Bitcoin come "hard money", si sottolinea la sua caratteristica di essere limitato in quantità e resistente all'inflazione, mentre

Easy money può riferirsi a valute tradizionali che possono essere create più facilmente e possono essere soggette a inflazione.

Hardened derivation

Livello: avanzato

Argomento: tecnologia

Esiste un caso speciale di derivazione delle chiavi, chiamata Hardened derivation. Un rapido promemoria: la funzione di derivazione ha due input, la chiave estesa e l'indice, che è un intero a 32 bit. Possiamo dividere questo spazio di 32 bit in due metà, sopra e sotto 231. È possibile ricavare chiavi private in entrambe le metà, ma solo la metà inferiore può essere utilizzata per ricavare chiavi pubbliche, ottenute mescolando la chiave privata del genitore nella formula se l'indice è superiore a 231.

Le chiavi private derivate con un indice della metà superiore sono chiamate chiavi Hardened e nel percorso di derivazione (la stringa di indici che viene utilizzata per la derivazione) sono indicate con il simbolo di primo ('), relativo a 231.

Esistono due possibili tipi di derivazione BIP32, Hardened o non-Hardened.

Nella notazione del percorso BIP32 standard, la Hardened derivation a un livello particolare è indicata da un apostrofo. Ad esempio, per i primi tre livelli viene utilizzato il seguente esempio di derivazione hardened, mentre per gli ultimi due livelli viene utilizzata la derivazione non hardened:

m / 44' / 0' / 1' / 1 / 33

Con le chiavi non-hardened, puoi provare che una chiave pubblica figlio è collegata a una chiave pubblica principale utilizzando solo le chiavi pubbliche.

Puoi anche derivare chiavi figlie pubbliche da una chiave padre pubblica, che abilita i wallet di sola visualizzazione. Con le chiavi figlio rafforzate, non è possibile dimostrare che una chiave pubblica figlio sia collegata a una chiave pubblica padre. Per motivi di sicurezza, l'utilizzo di hardened key è più sicuro, ma esistono casi d'uso per l'utilizzo di non-hardened key. Una chiave pubblica estesa padre insieme a una chiave privata figlio non protetta possono esporre la chiave privata padre. Ciò significa che le chiavi pubbliche estese devono essere trattate con maggiore attenzione rispetto alle normali chiavi pubbliche. È anche il motivo dell'esistenza di hardened key e del motivo per cui vengono utilizzate per il livello di account nell'albero. In questo modo, una perdita di chiavi private specifiche dell'account (o inferiori) non rischia mai di compromettere il master o altri account.

Hardware

Livello: base

Argomento: tecnologia

Sono dispositivi elettronici offline protetti da crittografia avanzata, garantita da componenti e standard di sicurezza molto alte, che rientrano nella categoria dei "cold wallet"

Hardware wallet

Livello: base

Argomento: tecnologia

Un hardware wallet è un dispositivo fisico che memorizza le chiavi private delle tue criptovalute in modo sicuro.
Le chiavi private sono ciò che ti consente di accedere e spendere le tue criptovalute.

Ci sono diversi tipi di hardware wallet disponibili, ma tutti funzionano in modo simile. Il dispositivo ha una schermata e alcuni pulsanti che vengono utilizzati per inserire alcune informazioni ed effettuare delle conferme, ad esempio la firma della transazione.

Gli hardware wallet sono considerati uno dei modi più sicuri per conservare le criptovalute perché le chiavi private sono memorizzate offline, il che le rende meno vulnerabili agli attacchi informatici.

Poiché tramite gli hardware wallet le chiavi private rimangono in possesso dell'utente, sono considerati non custodial.
Un hardware wallet solitamente è offline e per confermare e firmare le transazioni comunica con un dispositivo online e il software wallet generalmente tramite USB, in alcuni casi tramite Bluetooth o nfc, o QR code.

Sebbene tecnicamente connesso a Internet a volte, è ancora considerato un cold wallet o offline poiché le transazioni sono firmate all'interno del device senza esporre la chiave privata.
Ciò significa che la transazione è stata firmata offline prima di essere trasmessa ai nodi.

A causa di questa funzione di sicurezza, un eventuale malware nel computer o cellulare dell'utente non è in grado di accedere alla chiave privata e impossessarsene.

Gli hardware wallet più sicuri hanno un componente hardware chiamato secure element fornisce un ambiente sicuro e isolato per eseguire operazioni di crittografia e memorizzare in modo sicuro le chiavi private.

Molti hardware wallet si occupano anche della generazione delle chiavi, o meglio del seed dal quale generare le chiavi private. La generazione di chiavi private in un hardware wallet è un processo critico che richiede sicurezza e casualità per garantire l'assoluta segretezza della chiave.

La generazione avviene di solito quando un nuovo hardware wallet viene inizializzato, viene creato un seed e la Seed Recovery Phrase.

L'entropia utilizzata per la creazione del seed è fondamentale per la sua sicurezza, e generalmente gli hardware wallet basano i loro pseudorandom number generator (PRNG) su un oscillatore, un chip che ha una componente analogica che genera rumore.
A questo aggiungono altre fonti di entropia, quali input dell'utente, sensore di temperatura, sensore di movimento.

Hash

Livello: base

Argomento: tecnologia

Un hash è una funzione matematica crittografica che converte un dato di lunghezza arbitraria in una stringa di lunghezza fissa.

È una funzione fondamentale per i Bitcoin, e per la crittografia in generale. Gli hash sono usati ampiamente in Bitcoin: dalle strutture dati al mining, agli ID delle transazioni e gli indirizzi, e altro ancora.

Può essere considerata come una tecnica di crittografia in cui i messaggi vengono trasformati matematicamente in una sequenza di numeri e lettere di lunghezza fissa. Gli output hanno lunghezze impostate per rendere impossibile determinare la dimensione dell'input. Ad esempio, l'hash di una singola parola ha la stessa lunghezza dell'hash del testo di un intero libro.

Queste funzioni hash sono irreversibili, operano in una sola direzione, il che significa avendo l'input si otterrà sempre lo stesso hash, ma dall'hash è impossibile determinare quale sia il testo in input che genera quell'hash.

Ogni codice generato può essere considerato unico, il che significa che la possibilità che si possa avere lo stesso hash con due input diversi è infinitesimale e quindi trascurabile.

A cosa serve un codice segreto che non può essere decodificato? Innanzitutto, è un modo per verificare. Se vi viene inviato l'hash di un messaggio, non vi fornisce le informazioni necessarie per ricreare il messaggio. Ma quando ricevete il messaggio, potete inserirlo in un programma che genera l'hash, e se corrisponde esattamente all'hash ricevuto, si ha la certezza che il messaggio è quello originale e non è stato sostituito o alterato. È impossibile utilizzarlo per decodificare l'hash, ma è facile da utilzzare per effettuare la verifica.

Esistono numerosi algoritmi che realizzano funzioni hash con particolari proprietà che dipendono dall'applicazione. Nel caso di Bitcoin, la blockchain utilizza SHA 256 per generare un output lungo 256 bit (o 64 caratteri esadecimali), indipendentemente dalla dimensione dell'input. Nel mining di Bitcoin, questo input della funzione di hash corrisponde ad un numero da inserire in un insieme

di dati, ovvero l'header del blocco (potremmo dire la sua "intestazione"), in modo tale che una doppia esecuzione dell'hash SHA256 di tali dati sia un numero inferiore ad un target hash (valore espresso in nBits e proporzionale alla difficoltà della rete).

Hash Rate

Livello: intermedio

Argomento: tecnologia

L'Hash Rate indica la velocità con cui un computer è in grado di eseguire calcoli di hashing.

Nel contesto di Bitcoin e criptovalute, l'hash rate rappresenta l'efficienza e le prestazioni di una macchina per il mining.

Definisce la velocità di funzionamento di un hardware di mining quando si tenta di calcolare un hash di blocco valido. Il processo di mining prevede una miriade di tentativi di hashing, fino a quando non viene prodotto un hash valido. In altre parole, un miner di Bitcoin deve eseguire una serie di calcoli attraverso una funzione hash per produrre un hash e ha successo solo quando viene generato un determinato valore hash (un hash che inizia con un certo numero di zeri).

Pertanto, l'hash rate è direttamente proporzionale alla redditività di un miner o di un mining pool. Un hash rate più alto significa che la probabilità di estrarre un blocco è più alta e, quindi, il miner ha maggiori possibilità di ricevere la ricompensa del blocco.

Di solito, l'Hash rate della rete bitcoin aumenta: si aggiungono nuovi miner, e vengono immessi sul mercato hardware di mining con maggiore potenza di calcolo. Questo fa in modo che i blocchi vengano minati più velocemente.

Ci sono anche dei casi nei quali l'Hash rate diminuisce: ad esempio nel 2021 i miner cinesi che all'epoca erano la maggioranza, per motivi normativi hanno dovuto interrompere o spostare le loro attività, causando una forte diminuzione dell'Hash rate.

Un altro motivo per la diminuzione dell'Hash rate può essere dovuto ad un Bear market o Crypto winter che rende meno profittevole il mining fino a compromettere i bilanci dei miner costringendoli a spegnere le loro macchine o addirittura a chiudere.

Hashcash

Livello: avanzato

Argomento: economia

Hashcash è un sistema di Proof of Work (PoW) progettato nel 1997 da Adam Back per contrastare lo spam email e gli attacchi Denial-of-Service (DoS). Il

suo funzionamento si basa sull'obbligo di eseguire un calcolo computazionale prima di inviare un'email o effettuare una richiesta, rendendo economicamente svantaggioso lo spam su larga scala.

Come funziona Hashcash? Sfida crittografica: Per ottenere un "timbro" valido, il mittente deve generare un hash (es. SHA-1) di dati che includono l'indirizzo email del destinatario e un timestamp, con la condizione che l'hash risultante abbia un certo numero di zeri iniziali.

Proof of Work: Trovare tale hash richiede un processo di forza bruta (prova e errore), che consuma tempo e risorse computazionali. Una volta trovato, il timbro dimostra che il lavoro è stato svolto.

Rapporto con Bitcoin Bitcoin, creato da Satoshi Nakamoto nel 2008, adatta e potenzia il concetto di Hashcash nel suo meccanismo di consenso:

Ispirazione diretta: Satoshi cita esplicitamente Hashcash nel whitepaper di Bitcoin come base per il Proof of Work.

Consenso e sicurezza: In Bitcoin, i miner competono per risolvere un puzzle crittografico (hash con specifiche restrizioni) per validare transazioni e creare nuovi blocchi. Questo processo:

Protegge la rete: Renderla immune ad attacchi Sybil o doppie spese, poiché alterare la blockchain richiederebbe un'enorme potenza computazionale.

Regola la difficoltà: A differenza di Hashcash, la difficoltà del puzzle in Bitcoin si adatta dinamicamente per mantenere un intervallo di creazione dei blocchi di ~10 minuti.

Scalabilità e incentivi: Hashcash richiedeva un PoW minimo per singola azione (es. email), mentre Bitcoin lo scala a livello globale, legandolo a un sistema di ricompense (BTC) per incentivare i miner.

Il nonce nel blocco Bitcoin viene modificato per trovare l'hash corretto, simile alla ricerca del timbro in Hashcash.

Hashcash ha fornito le basi teoriche per il Proof of Work, che Bitcoin ha trasformato in un pilastro della sicurezza blockchain. La relazione è storica e tecnologica: senza Hashcash, il concetto di PoW in Bitcoin non sarebbe stato così rapidamente realizzabile.

Hashing

Livello: intermedio

Argomento: tecnologia

con hashing si intende il processo che genera un hash . hashing power o hash rate è la misura principale delle prestazioni di un miner di Bitcoin.

HD wallet

Acronimo di: Hierarchical Deterministic wallet

Wallet deterministici gerarchici

Livello: intermedio

Argomento: tecnologia

Un wallet può contenere al suo interno diversi indirizzi. Per diversi motivi anche legati alla sicurezza e alla privacy, è meglio evitare l'address reuse ovvero di avere un unico indirizzo sul quale gestire più transazioni, ma è opportuno usare diversi indirizzi, o coppie di chiavi (chiave privata e corrispondente chiave pubblica).

La generazione di diversi indirizzi al'interno dello stesso wallet inizialmente era effettuata generando in modo casuale i nuovi indirizzi, e risultava abbastanza scomoda, fino a quando con il BIP32 sono stati introdotti gli HD Wallet, dove la H sta per Hierarchical o gerarchico ovvero una serie di chiavi organizzate in modo gerarchico come in un albero, e la D sta per Deterministico ad indicare che le chiavi derivate non vengono generate in modo casuale ma attraverso una apposita funzione.

Le chiavi di questo albero vengono generate, o derivate, da una singola chiave che chiamiamo Master Key conosciuta anche come seed (seme). Questo meccanismo deterministico consente di poter generare tantissime chiavi, senza la necessità di fare il backup delle chiavi ogni volta che ne generiamo nuove ma mantenendo solo la copia del seed.

I wallet Hierarchical Deterministic, gerarchici deterministici, creati inizialmente per Bitcoin è stata successivamente adottata in molte altre cripto.

Gli HD Wallet per descrivere il modo con il quale vengono generate le nuove chiavi e come indentificarle, utilizzano una sequenza definita come Derivation Path

Per effettuare il backup di un wallet HD è quindi opportuno, oltre al seed, conoscere anche il derivation path.

Purtroppo le diverse implementazioni effettuate dagli sviluppatori di wallet non seguono le stesse modalità, nel corso del tempo sono nati degli standard che non sono adottati allo stesso modo dai produttori di wallet, e questo fa in modo che non sempre sia semplice o addirittura possibile ripristinare un back up da un wallet ad uno di un altro sviluppatore.

Helicopter Money

Livello: avanzato

Argomento: politica

Helicopter Money o helicopter drop si riferisce a un termine coniato per la prima volta da Milton Friedman in modo retorico per indicare gli effetti di qualsiasi meccanismo di trasmissione della politica monetaria tramite la distribuzione di contanti ai cittadini, come se fossero caduti da un elicottero durante la notte. Negli ultimi decenni questo termine è arrivato a riferirsi a un'applicazione figurativa della metafora di Friedman, come un tipo di strategia di stimolo monetario che aumenta la quantità dell'offerta di moneta e distribuisce direttamente denaro al pubblico per stimolare l'inflazione o l'aumento dei prezzi e crescita economica. Le politiche di Helicopter Money sono diventate una caratteristica comune della risposta dei responsabili politici agli shock economici su larga scala dal 2000.

Heuristic

Euristica

Livello: avanzato

Argomento: legale

In generale, un'euristica è un metodo approssimato per risolvere un problema.

Nel contesto della Chain Analysis, le euristiche sono utilizzate per dedurre relazioni tra gli indirizzi e le transazioni all'interno di una rete di pagamento basata su blockchain come Bitcoin.

In particolare, le euristiche vengono utilizzate per identificare e mappare gli indirizzi conosciuti, come quelli associati a Exchange, servizi di wallet, mixer, e servizi di darknet, e per ricostruire le relazioni tra indirizzi.

Le euristiche utilizzate in Chain Analysis possono essere suddivise in diverse categorie, tra cui:

- **Analisi degli indirizzi**: utilizzo di algoritmi per identificare gli indirizzi che appartengono a specifici gruppi o categorie, come gli indirizzi di scambio, Mining pool o i servizi di mixer di monete.
- **Analisi delle transazioni**: utilizzo di algoritmi per identificare le transazioni anomale o sospette, come le transazioni di grandi quantità di monete, le transazioni di monete mixate o le transazioni effettuate con indirizzi noti per attività illegali e basandosi su diverse proprietà delle transazioni, come Common Input, la dimensione delle transazioni, degli output e tra questi quelli che hanno importi tondi, i tempi di creazione delle transazioni, il tipo di script
- **Analisi delle relazioni**: utilizzo di algoritmi per identificare le relazioni tra indirizzi e transazioni, come le transazioni tra indirizzi appartenenti alla stessa entità o le transazioni tra indirizzi noti per attività illegali.
- **Analisi del contesto**: utilizzo di informazioni esterne alla blockchain, come i dati di geolocalizzazione o i dati sui prezzi delle criptovalute, per fornire un contesto per l'analisi delle transazioni e degli indirizzi.

Il loro utilizzo permette di fare delle inferenze sull'utilizzo degli indirizzi, ma questi non sono sempre precisi, poiché l'analisi euristica è basata su assunzioni. Alcune volte può essere ingannata da tecniche di privacy come il Coinjoin o Payjoin.

Hex

Acronimo di: Hexadecimal

Esadecimale

Livello: intermedio

Argomento: tecnologia

È un modo di rappresentare una cifra numerica o un contenuto digitale, che per i valori digitali consente una più comoda gestione rispetto alla rappresentazione decimale, perché ogni byte viene rappresentato da due cifre esadecimali.
Una stringa esadecimale è composta dai numeri 0 1 2 3 4 5 6 7 8 9 e dalle lettere A B C D E F senza distinzione tra maiuscole e minuscole.

Hierarchical channel

Livello: avanzato

Argomento: tecnologia

Gli Hierarchical channels, canali gerarchici, sono una proposta per l'implementazione di un nuovo tipo di Canali Lightning per accelerare e rendere più scalabile la Lightning Network.
Consentono un ridimensionamento flessibile, rapido e conveniente off-chain, senza transazioni on-chain che causano ritardi e costi aggiuntivi.

Il ridimensionamento dei canali on-chain può causare ritardi di diversi mesi e aumentare le commissioni. Le attuali proposte per il ridimensionamento dei canali off-chain coinvolgono la creazione di una Channel Factory o CoinPool e lo scambio di capacità tra canali all'interno della stessa Factory o Pool.
I canali gerarchici consentono un ridimensionamento flessibile off-chain senza richiedere uno scambio di capacità all'interno di un Pool limitato di utenti. I canali gerarchici consentono la creazione di un canale a due parti con due output principali, una per parte, più zero o più output HTLC, Hashed Time-Locked.

Ogni output da un canale gerarchico finanzia un altro canale che può essere visto come la radice di un albero off-chain di output in cui le foglie sono di proprietà di singoli utenti. Le parti possono utilizzare un HTLC per scambiare bitcoin, collegando i loro HTLC ad HTLC in altri canali (potenzialmente gerarchici), effettuando così pagamenti sul Lightning Network.

Con i canali gerarchici, gli sviluppatori propongono di risolvere due problemi:

- In primo luogo, consente un ridimensionamento flessibile, quasi istantaneo e off-chain, simile all'obiettivo della Lightning Network di consentire pagamenti quasi istantanei off-chain
- In secondo luogo, i canali gerarchici potrebbero essere utilizzati dagli utenti occasionali che possono inviare e ricevere bitcoin in modo privo di Watchtower, mentre gli utenti dedicati possono utilizzare tutta la loro capacità di canale per instradare i pagamenti, anche mentre l'utente occasionale è inattivo. I canali gerarchici consentirebbero agli utenti occasionali di operare in modo privo di Watchtower senza lasciare immobilizzato alcun capitale.

L'implementazione di canali gerarchici potrebbe contribuire a superare una delle maggiori limitazioni della Lightning Network, ovvero la sua scalabilità. Si prevede che i canali gerarchici forniranno il supporto necessario per i pagamenti efficienti sulla Lightning Network senza introdurre ulteriori ritardi, costi aggiuntivi e limitazioni di scalabilità. Lo sviluppo di canali gerarchici non richiede alcuna modifica al protocollo Bitcoin sottostante.

hodl invoice

Livello: avanzato

Argomento: tecnologia

Le hold invoices (richieste di pagamento in attesa), a volte chiamate hodl invoice, sono richieste di pagamento su Lightning Network in cui il destinatario non rilascia immediatamente il preimage al ricevimento di un pagamento. Invece, il destinatario esegue un'azione e poi accetta il pagamento, lo rifiuta esplicitamente o lo lascia scadere.

Ad esempio, Alice potrebbe generare automaticamente delle hold invoice sul suo sito web ma attendere che un cliente abbia effettivamente pagato prima di cercare nel suo catalogo l'articolo richiesto. Ciò le darebbe la possibilità di annullare il pagamento se non fosse in grado di consegnare.

Una hodl invoice attiva un flusso diverso sul lato del destinatario.
Invece di bloccare immediatamente e saldare l'htlc al momento dell'arrivo del pagamento, l'htlc per una hodl invoice viene solo bloccato e non ancora saldato. A quel punto, non è più possibile per il mittente revocare il pagamento, ma il destinatario può ancora scegliere se saldare o cancellare l'htlc e l'invoice'. Dal punto di vista del mittente, una richiesta di pagamento di una hodl invoice sembra identica a una normale richiesta di pagamento. Non c'è modo per il mittente di sapere quando una hodl invoice viene pagata.

Hold / Hodl

Livello: base

Argomento: finanza

In italiano il termine Hold, e Holder, viene spesso tradotto in "cassettisti", ovvero coloro che semplicemente comprano Bitcoin e continuano a detenerlo, qualunque cosa accada! In pratica, è una strategia con la quale si decide di tenere un asset a prescindere da qualsiasi evento accada, per un tempo deciso in precedenza.

Il termine HODL scritto con le lettere LD invertite è nato in modo del tutto casuale e divertente: la prima volta è apparso su un forum di discussione su Bitcoin nel 2013 e proveniva da un membro chiamato Game Kyuubi, che scrisse:
I AM HODLING
Dal contenuto del post, si è presunto che fosse ubriaco e volesse trasmettere la sua determinazione nel tenere i suoi BTC nonostante il pesante ritracciamento appena avvenuto.

Da allora, questo termine errato è diventato molto popolare nel mondo di Bitcoin e delle criptovalute in generale. Quindi, in sostanza, "HODL" era in origine nient'altro che un errore di battitura.

In seguito al termine si è attribuito il significato di acronimo per l'affermazione "hold on for dear life", il cui senso in italiano potrebbe essere *tieni duro e incrocia le dita*, o *tieni duro e con tutte le forze.*

Hold Invoice

Livello: intermedio

Argomento: tecnologia

è l'implementazione di un'estensione a una invoice Lightning in cui il passaggio finale di una risoluzione HTLC viene trattenuto dal destinatario del pagamento, in modo tale che il mittente del pagamento sia completamente committed, e annullato o eseguito in modo condizionale in un momento successivo. Una hodl invoice non è distinguibile da una normale ad un mittente del pagamento se non per il fatto che avrà un parametro di scadenza più lungo del normale.

Hop

Livello: intermedio

Argomento: tecnologia

Nelle reti informatiche, un hop è una connessione intermedia in una serie di connessioni o nodi che collegano due dispositivi.

Quando un elemento della rete, ad esempio un router o un gateway, è un dispositivo intermedio tra due host, nodi o reti diversi e remoti, è noto come hop.

Su Internet, la maggior parte dei pacchetti di dati deve passare attraverso diversi router prima di raggiungere la destinazione finale; questo passaggio viene

chiamato routing. Ogni volta che il pacchetto viene inoltrato al router successivo, si verifica un hop. Maggiore è il numero di hop, più lungo è il tempo che i dati impiegano per andare dalla sorgente alla destinazione.

Nel caso di Lightning Network, che è una rete composta di nodi che si collegano tra di loro attraverso channel o canali di pagamento, i pagamenti di solito attraversano più canali per raggiungere la loro destinazione. I nodi attraverso i quali il pagamento viene instradato sono definiti hop.

Tutte le reti di computer sono composte da molti nodi diversi. L'instradamento dei dati tra queste reti viene eseguito con una logica di instradamento tramite un router. Un router non solo esegue l'instradamento dei dati verso una rete, ma mantiene anche informazioni sui percorsi appresi da reti diverse.

In queste reti interconnesse, gli amministratori di rete hanno bisogno di vari strumenti di scoperta e gestione della rete per comprendere meglio il flusso dei dati e la loro gestione. A volte un amministratore desidera sapere quanti gateway sono presenti tra la sua rete e una rete remota o un sito web. Per garantire la comunicazione end-to-end, il pacchetto di dati potrebbe passare attraverso diversi router gateway nel suo percorso per raggiungere la destinazione. Ogni gateway che incontra nel suo percorso è noto come hop e il loro numero totale è noto come hop count.

Ping, traceroute e Trace Path sono comandi molto diffusi su Internet che vengono utilizzati per trovare gli hop (numero di gateway) tra la sorgente e la destinazione.

Hosted Wallet

Livello: intermedio

Argomento: legale

Con Hosted Wallet si intende un wallet di criptovalute che viene gestito da un fornitore di servizi finanziari, quali un CEX (exchage centralizzato). Viene anche definito come wallet custodial ma potrebbe essere più semplicemente definito come conto del cliente, perché non ha le funzioni proprie di un wallet di criptovalute. Per evidenziare che in questi tipi di wallet non si ha il controllo dei propri fondi si usa il detto Not Your Keys, Not Your Coins. Come contrapposizione, si intende unhosted wallet un wallet vero e proprio, non fiduciario del quale l'utente detiene la chiave privata e può gestire in autonomia i propri conti.

Il termine Hosted Wallet è diventato notorio a seguito delle votazioni del Parlamento europeo per imporre misure di regolamentazione per ostacolare le transazioni anonime di criptovalute.

Hot wallet

Livello: base

Argomento: tecnologia

Un hot wallet è un tipo di wallet connesso online. Grazie alla sua connessione alla rete, gli utenti possono effettuare transazioni in modo più immediato tuttavia questa facilità d'uso si accompagna a una maggiore vulnerabilità alla minaccia degli hacker, poiché la presenza online espone il wallet a potenziali rischi di sicurezza.

A differenza dei cold wallet, che sono dispositivi offline progettati per immagazzinare le criptovalute in un ambiente isolato dalla connessione internet, gli hot wallet offrono una maggiore convenienza a discapito di una sicurezza potenzialmente inferiore.

Pertanto, molti utenti scelgono di bilanciare la loro gestione di risorse digitali utilizzando una combinazione di hot e cold wallet.
Questa strategia consente loro di sfruttare i vantaggi della rapidità e dell'accessibilità della hot wallet quando necessario, mantenendo nel contempo una parte significativa delle loro risorse al sicuro in un ambiente offline tramite il ricorso alla cold wallet.

Howey Test

Livello: avanzato

Argomento: legale

L'Howey Test è un test che viene utilizzato per capire se una particolare operazione può essere considerata una Security, ovvero un contratto di investimento.

Negli Stati Uniti le Security devono essere registrate e autorizzate dalla SEC, Securities and Exchange Commission.

A giugno 2022 Gary Gensler, il presidente della SEC, parlando di criptovalute ha definito Bitcoin come commodity:
"*Alcune, come Bitcoin, e questo è l'unica che posso dire… sono commodities*"
di fatto escludendo che Bitcoin possa essere considerato security, ma ipotizzando che in linea di massima tutte le altre possano esserlo:
"*Dei circa 10.000 token presenti sul mercato delle criptovalute la stragrande maggioranza è costituita da security. Le offerte e le vendite di queste migliaia di security token sono coperte dalle leggi sulle security. Alcuni token potrebbero non soddisfare la definizione di security - quelli che chiamerò crypto non-security token. Questi rappresentano probabilmente solo un piccolo numero di token, anche se possono rappresentare una parte significativa del valore aggregato del mercato delle criptovalute.*"

L'Howey Test è un test legale sviluppato dalla Corte Suprema degli Stati Uniti nel 1946 nel caso SEC v. W.J. Howey Co.
Il test è stato creato per determinare se una transazione costituisce una Security ai sensi della legge federale degli Stati Uniti, in particolare la Securities Act del 1933 e la Securities Exchange Act del 1934.

Nel caso Howey, la società vendeva porzioni di frutteti di arance insieme a contratti per la gestione dei frutteti stessi. Gli acquirenti acquistavano non solo la terra, ma anche il servizio di gestione delle arance, con la promessa di ricevere profitti derivanti dalla vendita dei raccolti. La Corte Suprema ha stabilito che questo tipo di accordo costituisce un "contratto d'investimento" e quindi deve essere trattato come una security.

Secondo l'Howey Test, una Security si verifica quando sono presenti quattro elementi:

1. **Investimento di denaro**: Viene effettuato un investimento di denaro (o di beni materiali o servizi) da parte di un individuo.
2. **In una impresa comune**: L'investimento viene effettuato in una impresa comune, che si riferisce a un'organizzazione o a uno sforzo in cui il profitto è generato principalmente dallo sforzo altrui.
3. **Con l'aspettativa di profitto**: L'investitore si aspetta di ottenere un profitto dalla sua partecipazione o dagli sforzi altrui all'interno dell'impresa comune.
4. **A causa degli sforzi degli altri**: Il profitto dell'investitore dipende principalmente dagli sforzi degli altri, come i promotori o i manager dell'impresa comune.

Se tutti e quattro gli elementi sono presenti, la transazione viene considerata una Security e può essere soggetta alle leggi sulle securities negli Stati Uniti. Ciò significa che l'emittente dell'investimento potrebbe essere tenuto a registrare la sua offerta presso la Securities and Exchange Commission (SEC) e fornire informazioni complete e accurate agli investitori. Inoltre, gli investitori possono beneficiare di determinate protezioni previste dalla legge per gli investimenti in titoli.

L'Howey Test è stato spesso utilizzato nel tentativo di determinare se le criptovalute e le offerte iniziali di monete (ICO) rientrassero nella definizione di Security e quindi soggette alle normative statunitensi in materia di titoli di investimento.
La sua applicazione può variare in base al contesto e alla legislazione di altri Paesi, ma rappresenta comunque un punto di riferimento importante nella valutazione di transazioni che coinvolgono investimenti finanziari.

HTLC

Acronimo di: Hash Timelock Contracts

Livello: avanzato

Argomento: tecnologia

Un HTLC è un pagamento condizionale dal mittente al destinatario. Può essere speso immediatamente dal destinatario rivelando un certo codice segreto, oppure può essere reclamato dal mittente dopo un certo periodo di timeout.

Alla base di questo funzionamento c'è un concetto di base: il destinatario del pagamento può spenderlo subito attraverso una transazione valida, mentre la restituzione dell'importo al mittente è una forma di protezione per il mittente laddove il destinatario non pubblichi una transazione valida.

È quindi un pagamento temporizzato: il ricevente per incassarlo deve presentare un codice segreto, ma se non lo fa entro un certo tempo, il pagamento torna indietro a chi lo ha emesso.

È una funzione per creare smart contract, il cui uso più popolare è il Lightning Network di Bitcoin, e più recentemente DeFI attraverso l'uso di atomic swap sia sulla stessa chain che cross-chain, zero-knowledge contingent payment, and e altri protocolli di smart contract. Sono smart contract che facilitano le transazioni di scambio atomico, e funzionano come una "cassaforte virtuale" che richiede una chiave HashLock e TimeLock per sbloccare i fondi durante uno scambio.

HTLC è l'acronimo di "Hash Time-Locked Contract" (contratto bloccato da hash e temporale), ed è un tipo di smart contract utilizzato sulla rete Lightning per consentire il trasferimento di fondi tra due parti in modo sicuro e affidabile. Un HTLC stabilisce una condizione per il trasferimento di fondi, ad esempio il fornitore di liquidità deve fornire un hash di una password nota solo a lui, e il ricevente deve fornire la password corrispondente per ricevere i fondi. In questo modo, entrambe le parti hanno la certezza che l'altra parte ha rispettato i termini del contratto. Gli HTLC sono molto utili sulla rete Lightning perché consentono di eseguire transazioni in modo rapido e sicuro, permettendo ai partecipanti alla rete di fidarsi l'uno dell'altro senza dover passare attraverso intermediari centralizzati.

La funzione HTLC consente l'implementazione di transazioni vincolate a tempo tra due utenti: il destinatario di una transazione HTLC deve riconoscere il pagamento presentando una prova crittografica entro un periodo di tempo specificato (o più precisamente entro un numero di blocchi). Se il destinatario rinuncia o non richiede il pagamento, i fondi verranno restituiti al mittente originale. La funzionalità HTLC viene applicata nei canali di pagamento sia bidirezionali che instradati per consentire trasferimenti sicuri di fondi su vari canali, senza che sia necessario riporre fiducia su nessuno degli intermediari.

Le due componenti, o clausole, principali di un HTLC sono:

- una clausola di pagamento assicurata con un hashlock
- e una clausola di rimborso assicurata con un timelock.

La chiave hashlock assicura che la transazione vada a buon fine solo quando entrambe le parti forniscono una prova crittografica mentre la funzione timelock assicura che una scadenza possa essere impostata e rispettata per il completamento della transazione. Per aprire un hashlock e richiedere un pagamento, il destinatario deve rivelare la preimage di un digest di hash codificato nello smart contract. Per sbloccare un timelock e ricevere un rimborso, chi spende deve aspettare fino a un certo tempo codificato nello smart contract. Poiché le preimage

rivelate e il tempo trascorso non identificano in modo univoco la persona che dovrebbe ricevere il pagamento, gli HTLC sono sicuri solo se richiedono anche una firma unica che corrisponda alla chiave pubblica di chi spende (refundee) o del destinatario.

L'utilizzo sulla rete Lightning consente ai pagamenti Lightning di essere instradati attraverso più nodi. L'instradamento Lightning permette a due parti di effettuare transazioni in modo trustless senza un canale diretto tra loro, utilizzando invece canali intermediari.

I PTLC svolgono la stessa funzione degli HTLC ma possono fornire una migliore privacy, usare meno spazio a blocchi e prevenire l'intercettazione del routing, anche se hanno degli aspetti negativi.

Questo il codice script di un HTLC

```
# al destinario via LN penalty
OP_DUP OP_HASH160 <RIPEMD160(SHA256(revocationpubkey))> OP_EQUAL
OP_IF
    OP_CHECKSIG
OP_ELSE
    <receiver_htlcpubkey> OP_SWAP OP_SIZE 32 OP_EQUAL
        OP_NOTIF
            # al mittente via HTLC-timeout transaction (timelocked).
            OP_DROP 2 OP_SWAP <sender_htlcpubkey> 2 OP_CHECKMULTISIG
        OP_ELSE
            # al destinatario con preimage
            OP_HASH160 <RIPEMD160 (payment_hash)> OP_EQUALVERIFY
            OP_CHECKSIG
        OP_ENDIF
OP_ENDIF
```

HWI

Acronimo di: Hardware wallet interface

Livello: avanzato

Argomento: tecnologia

HWI, Hardware wallet interface o Interfaccia portafoglio hardware, è una libreria e uno strumento a riga di comando utilizzato per interfacciarsi con i wallet hardware utilizzando le PSBT Partially-Signed Bitcoin Transactions e i descrittori di script di output.

Progettata principalmente dagli sviluppatori di Bitcoin Core per consentire al software di utilizzare i wallet hardware come firmatari esterni, HWI viene ora utilizzata anche da altri wallet.

Hype

Livello: base

Argomento: finanza

È un termine che significa letteralmente “montatura” o “gonfiamento” ed è utilizzato per indicare la strategia di marketing atta a creare una forte aspettativa del pubblico, intorno a un determinato evento o prodotto. Molto spesso l’hype è voluto e pianificato, ma alle volte nasce spontaneamente da uno zoccolo duro di fan che non vedono l’ora di assistere a quel determinato evento o avere quel prodotto. Nelle criptovalute, viene sfruttato per aumentarne il prezzo oltre il reale valore di mercato, e così poterci poi speculare.

Hyperbitcoinization

Iperbitcoinizzazione

Livello: intermedio

Argomento: politica

La iperbitcoinizzazione è un processo per il quale una economia si basa principalmente o esclusivamente sulla valuta bitcoin. Il momento quando Bitcoin diventerà il principale mezzo di scambio andando a sostituire nella maggior parte degli scambi l’uso delle valute fiat. L’iperbitcoinizzazione è il punto di flesso in cui Bitcoin diventa il sistema di rappresentazione del valore predefinito del mondo. Man mano che sempre più individui e gruppi in tutto il mondo realizzano i vantaggi di un sistema digitale senza confini, resistente alla censura e nativo per la transazione di valore, una massa critica di utenti alla fine alimenterà la demonetizzazione della valuta e la sostituzione delle istituzioni finanziarie radicate del nostro mondo e delle potenze mondiali con un sistema più equo e pubblico. Poiché questo è un cambiamento fondamentale per il nostro mondo, le definizioni di hyperbitcoinization sono ampie e onnicomprensive.

I2P

Acronimo di: Invisible Internet Project

Livello: avanzato

Argomento: tecnologia

è un layer di rete anonimo (implementato come rete mista) che consente una comunicazione peer-to-peer resistente alla censura. Le connessioni anonime vengono ottenute crittografando il traffico dell’utente (utilizzando la crittografia end-to-end) e inviandolo attraverso una rete gestita da volontari di circa 55.000 computer distribuiti in tutto il mondo. Dato l’alto numero di possibili percorsi che il traffico può transitare, è improbabile che una terza parte guardi una connessione completa. Il software che implementa questo livello è chiamato “router

I2P" e un computer che esegue I2P è chiamato "nodo I2P". I2P è gratuito e open source ed è pubblicato con più licenze.

IBD

Acronimo di: Initial Block Download

Livello: intermedio

Argomento: tecnologia

La IBD, Initial Block Download o download iniziale della blockchain, è il processo tramite il quale un nuovo nodo, più precisamente un full node, che si unisce alla rete Bitcoin deve scaricare l'intera blockchain per convalidare tutte le transazioni nella rete. Questo è un passaggio fondamentale per la natura distribuita di Bitcoin poiché solo in questo modo un nodo può affermare di aver convalidato in modo indipendente tutte le transazioni.

Durante l'IBD, il nodo richiede copie di tutti i blocchi della blockchain ai suoi peer di rete e verifica che ogni blocco sia valido utilizzando l'algoritmo di consenso della rete Bitcoin.

Anche se i blocchi vengono richiesti a diversi nodi, il processo di IBD richiede di non fidarsi di nessuno perché un nodo potrebbe controllare i dati di diversi nodi e per la natura della catena di Proof-of-Work della blockchain.

Il nuovo nodo elabora questi blocchi e costruisce la blockchain fino a quando non si è aggiornato e sincronizzato con la rete.

Quando si inizia l'IBD, un nodo raccoglie prima tutti gli header dei blocchi da altri nodi e poi richiede ogni blocco completo. Questo viene fatto per aumentare l'efficienza e permettere agli utenti di iniziare a usare il loro nodo prima. Mentre si costruisce la blockchain blocco dopo blocco, un nodo Bitcoin costruisce anche l'insieme degli UTXO, o UTXO Set, la lista completa di tutti i bitcoin validi.

Poiché la blockchain di Bitcoin continua a crescere nel tempo, l'IBD può richiedere ore, giorni o settimane a seconda della larghezza di banda di internet e delle specifiche del computer.

Durante il processo di IBD, un nodo non accetta transazioni in entrata né richieste di transazioni mempool.

Una volta completata la fase di IBD, il nodo può iniziare a partecipare attivamente alla rete Bitcoin come peer che convalida le transazioni e contribuisce alla sicurezza della rete.

Per evitare di tenere tutta la blockchain su disco è possibile eseguire un nodo in una modalità definita Pruned mode.

Attraverso la proposta AssumeUTXO si sta predisponendo una modalità per consentire l'avvio di un full node senza la necessità di completare l'IBD.

Nel corso delle varie versioni di Bitcoin Core l'IBD ha avuto diverse evoluzioni:

- 0.3.2 Checkpoint
- 0.5.0 Saltata la verifica delle chechpointed signatures
- 0.8.0 passaggio a LevelDB e validazione parallela delle firme
- 0.10.0 Header-first sync
- 0.12.0 passaggio a libsecp256k1
- 0.14.0 AssumeValid
- 0.13.1 AssumeUTXO
- in futuro: UTREEXO

IBO

Acronimo di: Initial Bounty Offering

Livello: avanzato

Argomento: finanza

È il processo a tempo limitato attraverso il quale una nuova criptovaluta viene resa pubblica e distribuita a persone che investono tempo e abilità per guadagnare premi nella nuova criptovaluta, come fare traduzioni o marketing. A differenza di un'offerta di monete iniziale in cui è possibile acquistare monete, un IBO richiede un maggiore impegno mentale da parte del destinatario.

ICO

Acronimo di: Initial Coin Offering

offerta iniziale di monete

Livello: intermedio

Argomento: finanza

Il termine si richiama al più celebre IPO initial public offering, offerta pubblica iniziale più comunemente nota come quotazione in borsa, nella quale vengono emesse le azioni e messe in vendita al pubblico. Questo termine potrebbe rientrare nella definizione di crowdfunding o raccolta fondi: descrive una situazione in cui una soggetto raccoglie capitale emettendo token di criptovaluta, che sono venduti a un prezzo fisso, e ipoteticamente più conveniente, ai primi investitori. Questo termine ha poi generato delle specializzazioni quali ITO , IEO , IFO, STO , IDO .

IDO

Acronimo di: Initial DEX Offering

Livello: intermedio

Argomento: finanza

un successore di ICO e IEO, un nuovo modello di raccolta fondi completamente decentralizzato e senza autorizzazione per progetti crittografici, principalmente in DeFi, tramile il quale i token sono listati immediatamente dopo la vendita per il trading su uno scambio decentralizzato (DEX)

IEO

Acronimo di: Initial Exchange Offering

Livello: intermedio

Argomento: finanza

un metodo di raccolta fondi; un tipo di offerta pubblica di token ospitata e gestita da una piattaforma exchange per lo scambio di criptovalute. L'IEO si differenzia dalla ICO per il fatto che l'emissione e distribuzione dei token viene gestita da subito tramite un exchange.

Immutability

Immutabilità

Livello: base

Argomento: tecnologia

L'immutabilità può essere definita come la capacità di un Ledger blockchain di rimanere inalterato e invariato. Ciò significa che i dati conservati in una blockchain non possono essere modificati. Ogni blocco di informazioni come i dettagli della transazione utilizza un principio crittografico o un valore hash per mantenere inalterati i dati

Impermanent loss

Livello: avanzato

Argomento: finanza

È cio che avviene quando un liquidity provider ha una perdita temporanea di fondi a causa della volatilità in una coppia di trading.

Inbound Liquidity

Livello: avanzato

Argomento: tecnologia

La Inbound Liquidity, o liquidità in entrata, è la capacità di ricevere pagamenti bitcoin tramite Lightning Network e generalmente si riferisce ad un Canale Lightning.

Uno degli aspetti più impegnativi quando si avvia un nodo lightning è l'acquisizione di liquidità in entrata.

Può essere difficile da ottenere perché è necessario convincere un altro partecipante ad allocare capitale nella propria direzione prima di poter ricevere il pagamento. Questo può avvenire per buona volontà (chiedere a un amico), per caso (qualcuno che non conoscete ha scelto il vostro nodo per aprire un canale) o pagando direttamente per ricevere liquidità da un LSP, Lightning Service Provider.

La dimensione di un singolo pagamento sulla Rete Lightning è limitata dal balance (liquidity) dei canali nel percorso, che deve essere bloccato mentre il pagamento è in transito. Tuttavia, una volta che il pagamento è stato regolato, la liquidità può essere riutilizzata più volte, quindi se i pagamenti fluiscono in modo approssimativamente uniforme in entrambe le direzioni attraverso il canale, il volume totale dei pagamenti può facilmente superare la quantità di liquidità bloccata.

L'inbound liquidity è la quantità di fondi che sono disponibili per essere ricevuti da un canale Lightning Network. In altre parole, rappresenta la quantità di fondi che altri nodi possono inviare al nodo che possiede il canale in questione. L'inbound liquidity è uno degli elementi chiave del funzionamento di Lightning Network, poiché permette ai nodi di ricevere pagamenti e di partecipare alla rete e di eseguire transazioni.

Inbound routing fees

Livello: avanzato

Argomento: tecnologia

Inbound routing fees sono le fee che gli operatori dei canali di pagamento Lightning, addebitano per ricevere transazioni da altri operatori della rete.

In generale, le inbound routing fees si applicano quando una transazione proviene da un indirizzo non gestito direttamente dall'operatore che la riceve.

Queste fee sono utilizzate per coprire i costi associati alla ricezione e alla elaborazione di transazioni, comprese le spese di elaborazione, la gestione del rischio e la liquidità.

Il motivo per cui si vogliono le Inbound routing fees, è il seguente: supponiamo che stiate gestendo un nodo di routing stabile e che gestisca bene la propria liquidità. Si fa il rebalance e si ottiene un piccolo profitto. Ora un nodo che invia molti pagamenti, che chiamiamo *source*, apre un canale verso di voi, spingerà fuori tutta la liquidità outbound che avete in qualsiasi altro canale. Cercate di fare il rebalance, ma non è redditizio. Attualmente avete due opzioni:

- Aumentare le commissioni su tutti gli altri canali. In questo modo si blocca tutto il traffico proveniente da qualsiasi altro nodo, perché ora siete troppo

costosi.
- Chiudere il canale con la *source*. Perdendo un potenziale grande profitto.

Una soluzione a questo problema potrebbe essere rappresentata dalle Inbound routing fees. Probabilmente chiunque gestisca un nodo di routing e abbia vissuto la situazione di cui sopra è favorevole all'applicazione di Inbound routing fees in qualche forma. Se siete in grado di addebitare il traffico inbound, potreste essere in grado di gestire la tempesta di pagamenti dalla *source* senza influenzare gli altri percorsi di pagamento sul vostro nodo.

Inflation

Inflazione

Livello: base

Argomento: politica

Quando si parla di inflazione, nelle criptovalute, si pensa all'emissione ovvero alla creazione di nuove monete. E vero che, tecnicamente, anche le criptovalute sono soggette all'inflazione in relazione alla quantità emessa o minata, esattamente come avviene per l'oro e come avviene con le valute fiat ad esempio con il Quantitative Easing, ma l'inflazione si riferisce principalmente all'aumento del prezzo.

L'inflazione è il processo in seguito al quale le valute perdono valore nel tempo, causando un aumento dei prezzi dei beni di consumo. È un aumento generalizzato dei prezzi, determinato dall'aumento della domanda di beni e servizi rispetto all'offerta, e si traduce in un minore potere d'acquisto per la relativa valuta. L'inflazione è principalmente dovuta a un aumento costante della base monetaria o Quantitative Easing da parte del governo locale o della banca centrale, ma può essere causata dalla crescita dell'economia, dall'aumento del costo delle materie prime o dalla riduzione della domanda di denaro. Nelle criptovalute il valore di una criptovaluta può diminuire a causa della crescita della supply, e quindi dall'emissione di nuova criptovaluta, e alcune criptovalute seguono una politica inflazionistica fissa che diminuisce la circolazione dei token nel tempo. C'è una controparte alla coniazione di nuove monete: il burning, ovvero bruciarle togliendole così dalla circolazione. Per le stablecoin, il burning è particolarmente importante per mantenere l'offerta di token uguale al supporto patrimoniale che hanno.

Nelle economie moderne l'inflazione è un evento atteso. L'inflazione è generalmente misurata in base ai prezzi di beni e servizi, tracciati da un paniere di mercato medio ponderato di molte voci, noto come l'indice dei prezzi al consumo o CPI. Quando i livelli di inflazione sono estremamente alti, si parla di iperinflazione. L'iperinflazione si traduce in una rapida diminuzione del valore di una valuta, che è destabilizzante per un'economia e generalmente porta al collasso economico se il tasso di inflazione non può essere controllato. Livelli moderati di inflazione sono generalmente considerati dalla maggior parte degli

economisti salutari per un'economia. L'aumento pendente dei prezzi incentiva la gente a spendere soldi prima, stimolando il commercio. Tuttavia, l'inflazione significa che il valore di una valuta diminuirà costantemente nel tempo, rendendola una scarsa riserva di valore.

Inscription

Livello: avanzato

Argomento: tecnologia

Le Inscription degli ordinal Bitcoin sono i dati che vengono scritti, o inscritti, nella block chain bitcoin associati ad un satoshi, la più piccola unità di Bitcoin. Questi dati possono essere diversi tipi di contenuti digitali, quali testi, immagini, audio, video, un codice e altro.

Il processo di iscrizione degli Ordinals scrive o inscrive i dati del contenuto memorizzato nel witness della transazione Bitcoin, introdotto nell'aggiornamento SegWit della rete Bitcoin nel 2017. Il witness è una parte facoltativa della transazione Bitcoin che può essere utilizzata per memorizzare dati aggiuntivi.

Le Inscription negli ordinal Bitcoin sono simili aglii NFT, in quanto sono beni digitali non fungibili. Tuttavia, gli Ordinals hanno un vantaggio rispetto agli NFT tradizionali, in quanto sono memorizzati sulla blockchain di Bitcoin, che è una rete decentralizzata e immutabile.

Ecco alcuni esempi di dati che possono essere utilizzati come Inscription negli ordinal Bitcoin:

- Un testo: come un poema, una lettera o un codice sorgente
- Un'immagine: come una fotografia, un'opera d'arte o un meme
- Un video: come un film, un videoclip o un tutorial
- Un audio: come una canzone, un suono o un parlato
- Un codice: come un contratto intelligente o un programma software
- una pagina web: una pagina html visualizzabile con un browser web

Le Inscription negli ordinal Bitcoin possono essere utilizzate per una varietà di scopi, tra cui:

- Creare oggetti da collezione digitali unici.
- Registrare la proprietà di beni digitali.
- Certificare l'autenticità di documenti o opere d'arte.
- Creare sistemi di voto o di governance.

Le Ordinal Inscription di Bitcoin sono state introdotte a gennaio 2023 dallo sviluppatore Casey Rodarmor.

Un utilizzo popolare delle Inscriptions è la creazione di collezionabili digitali sulla rete Bitcoin chiamati "artefatti" (artifact). Pensateli come i collezionabili tradizionali, ad esempio le carte sportive. Una carta sportiva può essere preziosa

in base a una serie di fattori, tra cui la data di creazione, comunemente identificata da un numero di serie (in molti casi, più è stata stampata precocemente, più potrebbe essere preziosa) e la sua rarità.

Gli artefatti sono simili, solo che usano gli Ordinals per stabilire un numero di serie e le Inscriptions per allegare un'immagine. Ciò consente ai creatori di creare collezionabili sulla blockchain di Bitcoin. Se questo concetto vi sembra familiare, potrebbe essere perché sono simili agli NFT. Infatti, i collezionabili di artefatti sono conosciuti come NFT di Bitcoin.

Oltre ai collezionabili, i casi d'uso degli artefatti si stanno espandendo e sono stati utilizzati per supportare l'archiviazione di dati e i nomi di dominio, tra le altre funzioni.

Attraverso le Inscription è stato implementato lo standard BRC-20, che ha avuto un successo tale da costituire il caso d'uso più popolare degli Ordinal Inscription.

Cursed Inscriptions Le inscription vengono anche identificate in base ad numero, che gli viene assegnato in modo progressivo in base alla loro iscrizione nella blockchain bitcoin.

Le cursed inscription, in italiano "iscrizioni maledette", sono inscription che non hanno ricevuto un numero di iscrizione perché non sono state indicizzate e riconosciute dalle prime versioni del software Ord degli ordinal.

Il termine "maledetto" per le inscription è emerso quando è stato scoperto che alcune persone avevano utilizzato in modo inaccurato o intenzionalmente abusato di opcode per creare inscription, che hanno prodotto artefatti digitali che il software Ord non poteva identificare.

Le cursed inscription vengono create in quattro modi:

- Quando più inscription sono incluse in una singola transazione.
- Quando le inscription sono generate utilizzando opcode con numeri pari come OP_66.
- Quando numerose inscription sono legate a un singolo satoshi.
- Quando le inscription vengono fatte sull'input dopo il primo.

Mentre queste sono le principali modalità per creare cursed inscription, sono ancora in corso scoperte di ulteriori tipi di cursed inscription.

Il problema delle cursed inscription è stato sollevato per la prima volta ad aprile 2023. La soluzione temporanea è stata modificare il software Ord per riconoscere queste inscription non valide e assegnare loro numeri negativi a partire da -1.

Poco dopo che il problema è stato identificato, la comunità di Ordinals ha trasformato le cursed inscription in un'opportunità. Molti si sono affrettati a generare le prime 10.000 cursed inscription con l'assunzione che sarebbero state preziose.

L'aumento nella produzione intenzionale di cursed inscription ha portato al dibattito su se il team di Ordinals dovesse rilasciare un aggiornamento software che mantenesse i numeri di iscrizione negativi di questi asset.
Con il rilascio dell'aggiornamento v0.6.0 a giugno 2023, è stato permesso alle cursed inscription di mantenere i loro numeri negativi.
Con questo aggiornamento viene inclusa una attivazione chiamata Jubilee nel blocco 824544 (che potrebbe essere minato tra il 5 e il 6 gennaio 2023) che dovrebbe assegnare a tutte le nuove iscrizioni che in precedenza sarebbero state maledette numeri positivi. Questo aggiornamento le trasformerebbe in "blessed" (benedette). Tutte le cursed inscription precedenti a questo blocco dovrebbero mantenere i loro numeri negativi.

L'aggiornamento supporta un determinato sottoinsieme di cursed inscription, il che significa che il software di Ord riconosce ora tutte le oltre 71.000 cursed inscription, consentendone la negoziazione una volta che i mercati di Ordinals saranno stati aggiornati alla nuova versione del software.

Il secondo dibattito riguarda le cursed inscription generate utilizzando l'opcode OP_66. La discussione verte su se questi tipi di cursed inscription debbano essere inclusi nel set cursed o blessed. Il software di Ord non riconosce OP_66 e ha deliberatamente omesso gli opcode con numeri pari per lo sviluppo futuro.

Il team di Ordinals sta ancora valutando il supporto per le cursed inscription basate su OP_66. Pertanto, la v0.6.0 non supporta queste cursed inscription.

Secondo Rodarmor, supportare OP_66 e altri opcode con numeri pari non è la migliore idea, poiché le iscrizioni create con essi sarebbero svincolate. Ciò significa che non sarebbero collegate a uno specifico satoshi, rendendole non negoziabili e non trasferibili.

Intrinsic Value

Valore intrinseco

Livello: intermedio

Argomento: politica

La misura del valore di un determinato bene in base al valore che gli fornisce in sé e per sé, indipendentemente da altri fattori.

invoice

Livello: intermedio

Argomento: tecnologia

L'invoice è una richiesta di pagamento, la traduzione del termine potrebbe essere quello di fattura.

Nel caso delle Lightning Invoice, le invoice per la rete Lightning Network, il processo di pagamento sulla è avviato dal destinatario (beneficiario) che emette una invoice o richiesta di pagamento.

Le invoice includono l'hash del pagamento, l'importo, una descrizione e la scadenza.

Le invoice Lightning sono definite in BOLT #11. Le invoice possono anche includere un indirizzo Bitcoin di riserva a cui effettuare il pagamento nel caso in cui non si riesca a trovare un percorso, nonché suggerimenti per instradare un pagamento attraverso un canale privato.

IOU

Acronimo di: I owe you

Livello: avanzato

Argomento: finanza

L'acronimo IOU sta per "io ti sono debitore" e si riferisce a un documento informale che riconosce un debito che una parte ha nei confronti di un'altra, analogamente ad una cambiale. Il debito di solito comporta un valore monetario ma può anche essere correlato ad altri beni, come prodotti fisici o proprietà. A causa della qualità informale di queste cambiali, tendono a comportare un certo grado di incertezza e, a differenza delle obbligazioni e delle cambiali, non sono considerate uno strumento legale negoziabile. Ciò significa che la parte indebitata non ha alcun obbligo legale di pagare effettivamente il debito solo perché ha scritto e firmato un IOU. Possono essere semplici come un pezzo di carta o anche un accordo verbale tra membri della stessa famiglia. In alcuni casi, le aziende possono anche utilizzare gli IOU come metodo per registrare in modo informale quanto devono ad un'altra azienda o ai propri dipendenti, ad esempio. In sostanza, gli IOU non sono altro che note casuali che le persone creano per ricordare che devono pagare un debito in una data futura. A volte includono i nomi delle parti (o i nomi delle aziende), il valore, la firma e la data in cui sono stati creati. Tuttavia, in quanto documenti informali, gli IOU non includono alcuna informazione sulle conseguenze del mancato pagamento o sulle date specifiche in cui dovrebbe essere pagato.

IPFS

Acronimo di: InterPlanetary File System

file system interplanetario

Livello: intermedio

Argomento: tecnologia

È un protocollo attualmente utilizzato ad esempio per memorizzare i file collegati agli NFT, nato dalle tecnologie delle cripto, che offrire servizi alternativi o complementari al World Wide Web consentendo di avere caratteristiche quali decentralizzazione, immutabilità, incensurabilità, content addressing ovvero indirizzamento in funzione del contenuto e non location-based ovvero basato sulla posizione.

ITO

Acronimo di: Initial Token Offering

offerta iniziale di token

Livello: intermedio

Argomento: finanza

Simili alle ICO , ma l'obiettivo è l'offerta di token con utilità intrinseca comprovata (o ancora non dimostrata) sotto forma di software o utilizzo in un ecosistema.

JBOK

Acronimo di: Just-a-Bunch-of-Keys

Solo un gruppo di chiavi

Livello: intermedio

Argomento: politica

Un wallet di tipo JBOK, Just-a-Bunch-of-Keys, è una forma di wallet Bitcoin che genera casualmente nuove chiavi non correlate.

Questo tipo di wallet è definito anche come Wallet non deterministici.
In passato, i wallet JBOK erano ampiamente utilizzati ma sono stati superati dai Wallet HD o Wallet deterministici gerarchici, che offrono maggiore efficienza e comodità agli utenti.

Prima dell'introduzione dei Wallet HD o Wallet deterministici gerarchici, i wallet JBOK richiedevano un metodo di backup più complesso. Per eseguire il backup di un wallet JBOK, l'utente doveva salvare ogni singola chiave privata utilizzata dal wallet, il che poteva comportare un numero elevato e illimitato di chiavi da gestire. Questo processo di backup era laborioso e richiedeva uno sforzo significativo per garantire la sicurezza delle chiavi.

Con l'avvento dei wallet HD, è stato introdotto un approccio più efficiente al backup. Un wallet HD può essere sottoposto a backup tramite un singolo seed o seme o frase di recupero, che funge da punto di partenza per generare tutte le chiavi del wallet. Questo semplifica notevolmente il processo di backup, poiché

l'utente deve solo memorizzare il seed in un luogo sicuro. Inoltre, le chiavi estese fornite dai wallet HD offrono un'importante comodità agli utenti, consentendo loro di gestire e utilizzare tutte le chiavi generate a partire dal seed in modo più agevole.

Di conseguenza, i wallet JBOK sono stati gradualmente sostituiti dai wallet HD a causa della maggiore praticità e sicurezza offerte dai wallet deterministici.

JIT-Routing

Acronimo di: Just in Time Routing

Livello: avanzato

Argomento: tecnologia

Il Just-In-Time routing, o Instradamento Just-In-Time, è una proposta per consentire ad un nodo Lightning Network di riequilibrare due o più dei suoi canali in modo da avere fondi sufficienti per instradare un pagamento che altrimenti dovrebbe fallire.
Attualmente è solo una proposta.

JOMO

Acronimo di: Joy of Missing Out

Livello: intermedio

Argomento: finanza

Lo stato opposto di FOMO. Spesso usato dai non-possessori di criptomonete e da coloro che aprono posizioni in "short", che dichiarano la loro felicità di non essere coinvolti in criptovalute, di solito quando i prezzi sono in calo o viene rivelata una truffa.

justice transaction

Livello: avanzato

Argomento: tecnologia

Una Justice Transaction (transazione di giustizia) su Lightning Network, chiamata anche Penalty transaction, è una transazione che viene utilizzata per risolvere una disputa tra due parti che hanno aperto un canale di pagamento sulla rete Lightning.

Quando si apre un canale di pagamento sulla rete Lightning, viene creato uno smart contract tra le due parti, che stabilisce le regole per il trasferimento di fondi.

In caso di una disputa tra le due parti, ad esempio se una parte non onora lo smart contract, la Justice Transaction viene utilizzata per chiudere il canale e

assegnare i fondi alle parti secondo quanto previsto dallo smart contract nel caso una delle parti cerchi di imbrogliare.

La Justice Transaction è quindi un importante meccanismo di sicurezza della Lightning Network, che assicura la protezione dei fondi degli utenti in caso di eventuali problemi o dispute.

In un canale di pagamento sulla rete Lightning tra due parti, Alice e Bob, entrambe le parti devono mantenere i loro nodi online durante le transazioni per evitare che l'altro possa rubare i fondi in modo fraudolento.
Se una delle parti, ad esempio Alice, vuole tentare di rubare i fondi di Bob, deve chiudere il canale in modo non cooperativo senza il consenso dell'altra parte e scegliere un momento a lui favorevole, ad esempio quando l'altra parte non è online. Se queste condizioni sono soddisfatte, Alice trasmetterà un vecchio stato del canale che ha un saldo dei fondi a suo favore, sperando che Bob non si connetta o comunque non riesca a mandare on-chain la justice transaction entro il limite di tempo stabilito (tipicamente 24 ore) per correggere automaticamente la situazione.

Il nodo di Bob sa che la cronologia delle transazioni è diversa dalla revisione malevola di Alice, e se si connette entro il limite di tempo attiva il sistema di giustizia, e Alice sarà penalizzata perdendo tutti i Bitcoin che aveva depositato nel canale.

Il time-lock che impedisce per un tempo specificato a chi l'ha trasmessa di spendere i relativi output della transazione per un determinato tempo, consente all'altro partner, nel caso la transazione sia obsoleta, di avere tempo per pubblicare una Justice Transaction utilizzando il secret di revoca, che gli permette di punire il comportamento scorretto rivendicando tutti i fondi del canale per sé: la transazione di force close viene revocata (Revoked Lightning Force Close) con penalità (Force closed with penalty).

key path

Livello: avanzato

Argomento: tecnologia

In un wallet Bitcoin, il key path (o percorso chiave) è una stringa di numeri che identifica il percorso per una specifica chiave all'interno di un wallet gerarchico deterministico (HD).

Immagina il tuo wallet Bitcoin come un albero. La radice dell'albero è la chiave master, da cui vengono generate diverse chiavi secondarie. Ogni chiave secondaria può generare a sua volta altre chiavi secondarie, e così via. Il key path funge da mappa per navigare tra questo albero, specificando esattamente quale chiave secondaria (e le sue sottochiavi) si desidera utilizzare.

Il formato del key path dipende dal derivation path.
A volte i termini derivation path e key path sono usati in modo intercambiabile,

ma in realtà hanno sfumature di significato leggermente diverse: derivation path è il tipo di percorso che un wallet può supportare, e il key path è il percorso che consente di identificare una specifica chiave.

I componenti di un key path sono:

- Numero di livello: Indica la profondità della chiave secondaria nell'albero. La chiave master ha un livello 0, le sue chiavi secondarie di primo livello hanno un livello 1 e così via.
- Indice: All'interno di ogni livello, ogni chiave secondaria ha un indice univoco. L'indice inizia da 0.

Ad esempio, un key path di m/84'/0'/2'/0 indica:

- m: è la lettera iniziale che indica il tipo di master key. La lettera m minuscola indica master extended private key, o xprv, e la M maiuscola per i derivation paths per la xpub, la master extended public key.
- 84': a BIP84 P2WPKH / indirizzi SegWit nativi che iniziano con 'bc1'
- 0': Indica la prima chiave secondaria della chiave master. 2': La seconda chiave secondaria della prima chiave secondaria. 0: La prima chiave secondaria della seconda chiave secondaria.

I key path sono utilizzati in diversi contesti in un wallet Bitcoin:

- **Generazione di indirizzi**: La chiave privata identificata dal key path viene utilizzata per generare un indirizzo Bitcoin corrispondente. Questo indirizzo può essere utilizzato per ricevere Bitcoin.
- **Firma di transazioni**: La chiave privata viene utilizzata per firmare le transazioni Bitcoin, dimostrando la proprietà dei Bitcoin spesi e prevenendo la falsificazione.
- **Ripristino di un wallet**: Se si perde il dispositivo o il backup del wallet, è possibile utilizzare il key path per ripristinare il wallet da una seed phrase, una sequenza di parole che codifica la chiave master.

Con l'arrivo di Taproot, keypath assume un altro significato; i Bitcoin in un output P2TR possono essere spesi pubblicando una firma per una chiave pubblica, o soddisfando uno degli script contenuti nel nel merkle tree. La prima opzione è chiamata key path, mentre la seconda è chiamata script path.

Idealmente, gli output vengono spesi utilizzando il key path che impedisce agli osservatori di conoscere le condizioni di spesa di una moneta. Una spesa tramite key path potrebbe essere un "normale" pagamento da un wallet a firma singola o multipla o il regolamento cooperativo di un contratto multiparty nascosto.

Una spesa script path fa trapelare l'esistenza di un script path e che il key path non era applicabile, ad esempio perché le parti coinvolte non sono riuscite a raggiungere un accordo.

keychain

portachiave

Livello: intermedio

Argomento: tecnologia

Il termine inglese keychain in italiano significa portachiavi, ma per capirne l'uso nel contesto Bitcoin e critpovalute è più comprensibile se vengono tradotte le parole che lo compongono: key chiave, e chain catena.

Infatti generalmente si riferisce alla catena di chiavi tra loro collegate ad esempio gestite da un wallet HD, e quindi da un sistema capace di generare nuove chiavi in modo deterministico.

Si contrappongono ai wallet JBOK, Just-a-Bunch-of-Keys che può essere tradotto con "Solo un gruppo di chiavi", i Wallet non deterministici che ormai sono praticamente stati sostituiti da quelli deterministici.

KeySpend

Livello: avanzato

Argomento: tecnologia

Gli output (UTXO) Taproot si possono spendere in due modi: KeySpend e ScriptSpend. Con KeySpend si deve fornire la chiave, o meglio una firma bip-schnorr per la chiave pubblica nell'output.

Contrariamente ai precedenti formati delle transazioni Bitcoin, l'output di Taproot non distingue tra un public KeySpend path e uno ScriptSpend path. È sempre come un public key path: scriptPubKey contiene un programma testimone composto da due elementi:

- SegWit version: 1
- 32-byte witness program, chiave pubblica TapRoot codificata secondo le regole BIP340

Quindi ogni transazione TapRoot è una transazione P2TR Pay-to-TapRoot.

Se c'è un solo soggetto che controlla un'output TapRoot, si può utilizzare un Public KeySpend Path. Questo è il modo più semplice per spendere l'output di TapRoot.

Un altro caso di Public KeySpend Path è un accordo di collaborazione reciproca tra tutte le parti controllanti. In questo caso, tutte le parti creano in modo collaborativo la firma aggregata della transazione utilizzando le loro chiavi private indipendenti, che sono state precedentemente utilizzate per creare la chiave pubblica aggregata, definita nel programma witness dell'output.

Indipendentemente dalla possibilità di utilizzare il public key path per spendere l'output di P2TR, ci può essere un altro modo per spendere: uno script path.

Può essere utilizzato come caso di ripiego quando la spesa collaborativa è impossibile. Un singolo script o molti script organizzati nel Merkle tree possono essere utilizzati per coprire molti scenari diversi.

La differenza principale delle transazioni Taproot rispetto alle transazioni Bitcoin convenzionali è che gli script che controllano le monete sono contenuti all'interno di una struttura ad albero chiamata ramo tapScript che è impegnata privatamente nella transazione. Questi script non hanno bisogno di essere rivelati se il percorso (path) KeySpend viene utilizzato per spostare le monete. Mentre una transazione convenzionale richiede che l'intero script sia rivelato, una transazione Taproot può essere spesa con una chiave che evita di rivelare gli script e se il percorso KeySpend non è fattibile, solo la parte eseguita dello script viene rivelata sulla blockchain. Tutti gli altri percorsi degli script possono rimanere privati, o essere rivelati selettivamente off-chain.

KYC

Acronimo di: Know Your Client

Conosci il tuo cliente

Livello: base

Argomento: legale

Il KYC rappresenta una delle principali minacce ai principi che hanno ispirato la creazione e lo sviluppo di Bitcoin, compromettendo la sua indipendenza.

L'acronimo KYC, che sta per "Know Your Customer" (Conosci il tuo cliente), ha avuto origine nel settore bancario come un insieme di procedure e processi adottati dalle istituzioni finanziarie per verificare l'identità dei propri clienti. Progressivamente, queste pratiche sono state estese a entità come CEX e altri operatori del mondo Bitcoin e delle criptovalute. Tali procedure richiedono la raccolta di dettagliate informazioni personali, come nome, indirizzo e dati fiscali, compromettendo la natura pseudonima di Bitcoin.

Il KYC rappresenta una minaccia significativa per Bitcoin su vari aspetti fondamentali:

- **Privacy**: L'originale concezione di Bitcoin mirava a consentire transazioni finanziarie peer-to-peer senza intermediari centrali. L'introduzione del KYC viola la privacy richiedendo la divulgazione di informazioni personali sensibili.
- **Rischi di sicurezza**: Le informazioni del KYC sono spesso raccolte in database noti come "data silos", e nel corso del tempo si sono verificati molti casi di violazione e pubblica diffusione di tali dati, comportando gravi rischi:

  - **Furto di identità**: L'accesso alle informazioni KYC può essere utilizzato per frodi o furto di identità, inclusa l'apertura di account finanziari falsi.
  - **Phishing e attacchi mirati**: Le informazioni ottenute da una violazione di dati KYC possono essere sfruttate per attacchi mirati, come e-mail di phishing personalizzate per ottenere ulteriori informazioni sensibili.
  - **Estorsione**: Se i dati KYC includono informazioni particolarmente sensibili, gli attaccanti potrebbero cercare di estorcere denaro o compiere altre azioni dannose minacciando di divulgare tali informazioni o conoscendo la residenza dell'utente effettuare minacce alla persona e ai suoi familiari.
  - **Molestie**: la conscenza del patrimonio di un individuo, o anche solo l'idea che un individuo abbia una certa disponibilità di risorse, lo espone a molestie sia da parte di conoscenti che sconosciuti

- **Decentralizzazione**: Il concetto di decentralizzazione è fondamentale per Bitcoin. Il KYC, spesso implementato da istituzioni centrali e governi, può andare nella direzione della centralizzazione, poiché le informazioni vengono raccolte e gestite da entità centrali.
- **Resistenza alla censura**: Bitcoin è progettato per essere resistente alla censura e alle interferenze centralizzate. L'implementazione del KYC potrebbe essere vista come un modo per esercitare un controllo centralizzato sulle transazioni, e potrebbe compromettere la capacità di Bitcoin di resistere a eventuali tentativi di censura finanziaria. In tal modo, il KYC diventa anche uno strumento nelle mani dei governi per combattere avversari politici.

Il KYC viene spesso associatà alla presunta necessità di effettuare attività AML.

Shotgun KYC Un comportamento ancora più subdolo è quello definito *KYC shotgun* (traducibile come "a sorpresa"): si verifica quando una piattaforma consente la registrazione di un account senza richiedere il KYC, permettendo all'utente di depositare i propri fondi in criptovaluta.
Tuttavia, quando l'utente desidera prelevare i fondi, la piattaforma impone il KYC, che può richiedere tempi lunghi per essere completato.
In questi casi, possono anche esserci situazioni in cui il KYC non viene completato positivamente, impedendo all'utente di prelevare i propri fondi.

KYT

Acronimo di: Know Your Transaction

Livello: intermedio

Argomento: legale

è un processo utilizzato dagli istituti finanziarie per monitorare le attività dei commercianti-clienti attraverso l'analisi dei dati delle loro transazioni. L'esame dei dati delle transazioni consente di trarre conclusioni accurate e basate sui dati, in quanto produce le prove essenziali richieste in caso di sospetti su qualsiasi attività commerciale fraudolenta. Questo processo serve per mettere in guardia l'istituto sulle eventuali attività illecite, oppure ed è utilizzato per controllare eventuali attività di (AML). Il KYT può essere richiesto dopo il KYC.

lamport signatures

Livello: avanzato

Argomento: tecnologia

Una lamport signature, nota anche come firma digitale Lamport, è un tipo di firma digitale ideata da Leslie Lamport nel 1979.
Le firme Lamport sono basate su funzioni hash one-way e sono progettate per essere efficienti e sicure.

In parole semplici, una firma Lamport consente a un utente di firmare un messaggio in modo che chiunque possa verificare che il messaggio provenga effettivamente da quell'utente e che non sia stato manomesso.

Le chiavi pubbliche di Lamport sono costituite da due elenchi di hash digest. Le firme Lamport sono costituite dalle preimmagini per gli hash selezionati. Un programma condiviso tra il firmatario e il validatore interpreta quali preimmagini vengono rivelate come istruzioni.

Laser eyes

Livello: base

Argomento: politica

Una moda tra i bitcoiner, per riconoscersi tra loro, cambiando o modificando le immagini del proprio profilo per far sembrare che i loro occhi emettano raggi laser. E' stato usato per promuovere l'idea che il valore di un bitcoin arriverà a $100k

lattice

reticolo

Livello: avanzato

Argomento: tecnologia

In matematica, e in particolare in geometria e in teoria dei gruppi, un reticolo, in inglese lattice, è un sottogruppo discreto che genera lo spazio vettoriale reale.

Nel contesto della crittografia, gli algoritmi basati sui reticoli, o lattice-based algorithms, sono spesso utilizzati per la crittografia a chiave pubblica.
Questi algoritmi sfruttano problemi matematici difficili, come il problema del reticolo di approssimazione più vicino (Closest Vector Problem, CVP) o il problema del sotto-reticolo (Learning With Errors, LWE), che si pensa siano computazionalmente intrattabili.

Tuttavia, gli attacchi basati sui reticoli cercano di sfruttare eventuali debolezze o vulnerabilità presenti nell'implementazione o nelle configurazioni specifiche degli algoritmi basati sui reticoli per rompere la sicurezza crittografica.

lattice-based attack

attacco basato sui reticoli

Livello: avanzato

Argomento: tecnologia

Un attacco basato sui reticoli (lattice-based attack) è un tipo di attacco crittografico che sfrutta le proprietà matematiche dei reticoli per violare la sicurezza di un sistema crittografico. Un reticolo è una struttura matematica bidimensionale o tridimensionale composta da un insieme di punti allineati in una griglia regolare.

È stato dimostrato che con alcune particolari condizioni Bitcoin può essere vulnerabile all'attacco basato sui reticoli, è tale attacco è stato utilizzato per molti anni per svuotare centinaia di indirizzi Bitcoin compromessi.

Nel contesto della crittografia, gli algoritmi basati sui reticoli sono spesso utilizzati per la crittografia a chiave pubblica. Questi algoritmi sfruttano problemi matematici difficili, come il problema del reticolo di approssimazione più vicino (Closest Vector Problem, CVP) o il problema del sotto-reticolo (Learning With Errors, LWE), che si pensa siano computazionalmente intrattabili. Tuttavia, gli attacchi basati sui reticoli cercano di sfruttare eventuali debolezze o vulnerabilità presenti nell'implementazione o nelle configurazioni specifiche degli algoritmi basati sui reticoli per rompere la sicurezza crittografica.

Gli attacchi basati sui reticoli possono essere di varie forme, tra cui:

1. **Attacchi algoritmici**: cercano di sfruttare debolezze nell'algoritmo stesso per ottenere informazioni sensibili o rompere la crittografia.
2. **Attacchi di implementazione**: mirano a sfruttare le vulnerabilità nella realizzazione pratica dell'algoritmo, come ad esempio la gestione errata delle chiavi o degli errori di programmazione, per ottenere accesso non autorizzato.
3. **Attacchi laterali** (Side-channel attacks): sfruttano le informazioni ottenute misurando il consumo di energia, il tempo di esecuzione o altre

informazioni accessorie durante il processo di crittografia per inferire la chiave segreta.

4. **Attacchi quantistici**: cercano di utilizzare le potenziali capacità di un computer quantistico per risolvere i problemi matematici dei reticoli in modo efficiente, minando così la sicurezza degli algoritmi basati sui reticoli.

Nel caso di Bitcoin, è ben noto nella comunità crittografica che lo schema di firma ECDSA è fragile rispetto alle vulnerabilità nella generazione dei nonce. Un attaccante può recuperare la chiave privata ECDSA di un firmatario se conosce il nonce utilizzato per generare una singola firma; se un firmatario firma due messaggi distinti con lo stesso nonce; se un firmatario firma più messaggi con nonce inaspettatamente brevi; se l'attaccante può apprendere i bit più significativi di molti nonce di firma, e così via.

Layer 2

Livello: base

Argomento: tecnologia

Il significato esatto di layer 2, in italiano livello 2 o più raramente secondo strato, applicato a Bitcoin non è perfettamente definito e condiviso.

Con livello 2 generalmente ci si riferisce a un protocollo secondario basato sul sistema blockchain di Bitcoin.
Layer 2 dovrebbe rappresentare una soluzione di scaling che consente un elevato throughput di transazioni ereditando completamente la sicurezza della blockchain sottostante su cui è costruita.

L'obiettivo principale di questi protocolli è quello di migliorare la scalabilità Bitcoin, in termini di numero di tps, o transazioni al secondo, la velocità di conferma delle transazioni.

Queste soluzioni sono anche note come soluzioni di scalabilità off-chain perché le transazioni possono essere scambiate senza la necessità di salvare ogni singola transazione sulla blockchain.
In questo modo le soluzioni di livello 2 hanno il potenziale per raggiungere un elevato throughput senza sacrificare la sicurezza della rete che si appoggia alle caratteristiche di sicurezza della blockchain.
In altre parole, gran parte del dettaglio degli scambi può essere spostato sul secondo livello. Così, mentre la catena principale (livello 1) garantisce la sicurezza, il secondo livello offre un elevato throughput, essendo in grado di eseguire centinaia, o addirittura migliaia, di transazioni al secondo.

Per risolvere il problema del collo di bottiglia descritto sopra, sono state lanciate soluzioni di livello 2 per alleggerire la pressione sulla blockchain principale. Le soluzioni di livello 2 permettono di astrarre le transazioni dalla blockchain sottostante, consentendo di elaborare migliaia di transazioni al secondo.

La soluzione Bitcoin più conosciuta di livello 2 è Lightning Network.
Altre soluzioni di livello 2 sono i Zk-Rollup o rollup a conoscenza zero (Zero-Knowledge) e i rollup ottimistici.

Ledger

Libro Mastro

Livello: base

Argomento: tecnologia

Il termine ledger, in italiano registro o libro mastro, viene utilizzato spesso come sinonimo di blockchain.

Un ledger rappresenta un registro digitale immutabile e decentralizzato che registra tutte le transazioni effettuate all'interno di una specifica rete blockchain. Questo registro è distribuito tra i nodi della rete, e ogni nodo conserva una copia identica e aggiornata del ledger. Questa duplicazione e distribuzione del ledger tra i nodi contribuisce a garantire la sicurezza, l'integrità e la resistenza alla censura della blockchain.

Le transazioni vengono inserite in questo ledger in blocchi, seguendo regole di consenso che garantiscono che le informazioni registrate siano verificate e condivise in modo affidabile. Una volta che una transazione è registrata nel ledger, diventa parte permanente della catena dei blocchi e non può essere alterata o cancellata, rendendo le transazioni immutabili.

La trasparenza della blockchain consente a chiunque di accedere e verificare le transazioni registrate nel ledger, senza bisogno di autorizzazioni o intermediari. Questa caratteristica è fondamentale per la fiducia e la sicurezza nella rete, poiché permette la verifica delle transazioni da parte di qualsiasi parte interessata.

Va notato che, sebbene "ledger" sia un termine comunemente associato alle blockchain, è anche il nome di una società che produce hardware wallet con lo stesso nome. Tuttavia, nel contesto delle blockchain, il termine si riferisce principalmente al registro digitale delle transazioni.

legacy

Livello: base

Argomento: tecnologia

Quando si parla di Legacy in Bitcoin, generalmente ci si riferisce a pratiche e formati che sono anora supportati ma che sono state superate da nuovi standard.

Può riferirsi a:

- indirizzi, legacy address

- transazioni
- blocchi
- script o altri elementi.

In tutti questi casi, quando si parla di legacy generalmente ci si riferisce al formato utilizzato prima dell'introduzione di SegWit che ha cambiato la rappresentazione degli indirizzi, le transazioni e i blocchi, pur mantenendo la compatibiità con i formati precedenti.

Legacy address

Livello: base

Argomento: tecnologia

Gli indirizzi Legacy sono quelli definiti nel protocollo iniziale del bitcoin e usati inizialmente.

Sono riconoscibili perché iniziano con il numero 1, e a questi si sono aggiunti quelli che iniziano con 3.

La codifica utilizzata per questo tipo di indirizzi è base58.

Con l'aggiornamento SegWit nel 2017, agli indirizzi Lgacy si sono aggiunti gli indirizzi che iniziano con bc1 conosciuti anche come Bech32, e si stanno diffondendo progressivamente grazie alle loro caratteristiche più avanza e alla possibilità di effettuare

Legal tender

Corso legale

Livello: intermedio

Argomento: politica

La valuta a corso legale è qualsiasi cosa riconosciuta dalla legge come mezzo per saldare un debito pubblico o privato o soddisfare un obbligo finanziario, compresi i pagamenti delle tasse, i contratti e le multe legali o i danni. Praticamente ogni paese ha la sua valuta a corso legale. Un creditore è legalmente obbligato ad accettare valuta a corso legale per il rimborso di un debito.

Il corso legale è il denaro legalmente riconosciuto all'interno di una data giurisdizione politica. Le leggi sul corso legale impediscono effettivamente l'uso di qualsiasi cosa diversa dal corso legale esistente come denaro nell'economia. Il corso legale serve le funzioni economiche del denaro più alcune funzioni aggiuntive, come rendere possibile la politica monetaria e la manipolazione della valuta. Dal 2021 lo stato di El Salvador ha dichiarato Bitcoin valuta a corso legale, in aggiunta al dollaro Una valuta fiat è qualsiasi tipo di valuta emessa dal governo che è usata come valuta a corso legale dai cittadini e dal governo di una specifica nazione o regione.

Leverage / Gearing

Leva finanziaria

Livello: intermedio

Argomento: finanza

La Leva Finanziaria si riferisce al prestito che trader prende da un intermediario, consentendogli di ottenere un'esposizione molto maggiore rispetto a quella consentita dal suo capitale. La leva viene utilizzata dagli investitori per aumentare il proprio potere d'acquisto sul mercato, durante operazioni di Marging Trading. La leva finanziaria ha l'effetto di moltiplicatore i propri capitali, e quindi i guadagni ma anche le perdite.

Il Marging Trading è eccezionalmente rischioso, e può esserlo ancora di più nel settore delle criptovalute a causa delle forti oscillazioni del prezzo. Questo rischio aumenta ulteriormente nel caso degli exchange di criptovalute poiché alcuni possono consentire delle leve finanziarie con valori molto più alti rispetto ai mercati regolamentati.

Come esempio, se prendiamo una posizione di $100 in Bitcoin, supponendo che la posizione di un trader sia stata aumentata con una leva di 10x (10 volte), comunemente espressa come un rapporto di 1:10, significa che dalla disponibilità iniziale di $100 BTC del trader viene concessa dall'exchange una disponibilità di $1000. L'importo che il trader ha inizialmente viene chiamato Margin. Questo importo viene utilizzato come collaterale, e se il valore della criptovaluta scende al punto in cui le perdite sono paria al collaterale, la posizione viene liquidata (in pratica c'è il rischio di perdere tutto).

La quantità di leva a cui un investitore può accedere dipende dalla piattaforma di trading scelta, nonché dall'asset digitale a cui desidera acquisire esposizione. Alcuni paesi hanno cercato di porre un freno al Margin Trading, temendo che potesse causare ingenti perdite tra gli investitori meno esperti.

Liberty Reserve

Livello: avanzato

Argomento: economia

Liberty Reserve era una piattaforma di valuta digitale che permetteva trasferimenti di denaro tra utenti, ma non consentiva rimborsi.

Liberty Reserve è stato un servizio di trasferimento di denaro online centralizzato con sede in Costa Rica, consentiva agli utenti di tutto il mondo di trasferire denaro tra loro in modo anonimo e con commissioni minime.

Fondato nel 2006 in Costa Rica come servizio di trasferimento di denaro online.

Nel 2013 le autorità statunitensi chiedono a Liberty Reserve di chiudere i battenti con l'accusa di riciclaggio di denaro e gestione di un'attività di trasmissione

di denaro senza licenza. Le autorità hanno anche accusato Budovsky di aver riciclato milioni di dollari attraverso il servizio. Liberty Reserve è stata chiusa e Budovsky è stato arrestato.

Nel 2016 il fondatore di Liberty Reserve, Arthur Budovsky, si dichiara colpevole di un'accusa di riciclaggio di denaro e viene condannato a 20 anni di prigione.

Per quanto riguarda il suo rapporto con Bitcoin, Liberty Reserve era utilizzata come uno dei metodi per trasferire fondi verso e da scambi di Bitcoin, come Mt. Gox o TradeHill. Ad esempio, c'erano servizi che permettevano di trasferire fondi da Liberty Reserve a questi exchange.

Tuttavia, è importante notare che ci sono stati problemi legati alla sicurezza e all'affidabilità di alcuni metodi di pagamento, incluso Liberty Reserve, che ha congelato i fondi di alcuni clienti fino a quando non sono stati verificati.

Liberty Reserve era un servizio centralizzato, mentre Bitcoin è una rete decentralizzata. Ciò significa che Liberty Reserve era controllato da una singola entità, mentre Bitcoin è gestito da una rete di utenti in tutto il mondo.

Anonimato: Liberty Reserve offriva un elevato grado di anonimato, ma non era completamente anonimo. Le autorità sono state in grado di rintracciare alcune transazioni. Bitcoin offre un certo grado di anonimato, ma le transazioni sono registrate su un libro mastro pubblico (blockchain) e possono essere tracciate.

Light Client

Livello: base

Argomento: tecnologia

Un Light Client, o lightweight client, è un client Bitcoin che interagisce con la rete Bitcoin interrogando i nodi per specifiche transazioni e informazioni sui blocchi, ma non scarica e archivia l'intera blockchain.

Tipicamente utilizzato dai wallet come un modo per accedere alle informazioni sul saldo e sulle transazioni senza richiedere la significativa memoria necessaria per mantenere un nodo completo.

Lightning Channel

Canale Lightning

Livello: base

Argomento: tecnologia

La rete Lightning Network è composta da migliaia di canali di pagamento bidirezionali, noti come canali Lightning.

Un canale Lightning è una connessione tra due parti attraverso la quale le transazioni lightning vengono inviate avanti e indietro, e queste transazioni ricalibrano i saldi bitcoin di ciascuna parte all'interno del canale.

A grandi linee, il ciclo di vita di un canale consiste in:

- **Apertura** del canale attraverso una Funding Transaction, la transazione on-chain che fornisce liquidità al canale bloccando i bitcoin nella blockchain e spostandoli virtualmente nel canale;
- **Pagamenti** che vengono effettuati tramite transazioni off-chain provvisorie chiamate Commitment Transaction che spostano la liquidità all'interno del canale e non vengono trasmesse singolarmente nella blockchain;
- **Chiusura** del canale che può essere:
  - **Collaborativa**, effettuata tramite la Closing Transaction, la transazione di chiusura che gestisce i diversi casi di chiusura collaborativa;
  - **Non-Collaborativa** ,forzata o di difesa dal furto con transazioni di revoca, chiamata anche force close.

Ad esempio i due partner Alice e Bob decidono di aprire un canale Lightning e costruiscono in modo cooperativo un indirizzo multisig 2-of-2. Qualsiasi bitcoin inviato a questo indirizzo richiede due firme, una da ciascuna parte, per essere speso: Alice e Bob aprono un canale e depositano 1 BTC ciascuno. Se Alice desidera pagare Bob 0,5 BTC, firma una spesa di transazione dall'indirizzo multisig. Questa transazione ha due output: Bob riceverà 1,5 BTC e Alice riceverà 0,5 BTC. Poiché la spesa dall'indirizzo multisig richiede due firme, questa non è ancora una transazione valida e Alice non può trasmetterla alla rete Bitcoin. Invece, invia la transazione parzialmente firmata, la commitment transaction, a Bob, che la conserva ma non la trasmette. Alice ha pagato a Bob 0,5 BTC, ma Bob non ha saldato questo pagamento alla blockchain di Bitcoin. Questo è il motivo per cui le transazioni Lightning sono così economiche: non richiedono che i miner confermino ogni transazione inserendola in un blocco della blockchain.

Un canale può rimanere aperto per tutto il tempo in cui il nodo che collega i peer rimane online e nessuno dei due peer sceglie di chiudere il canale.

Gli utenti possono aprire più canali tra loro, noti come canali duplicati, per poter fare transazioni per diversi scopi, o per aumentare le probabilità di avere capacità di instradare i pagamenti verso l'altra parte.

Sarebbe inefficiente se gli utenti dovessero aprire un canale con tutti quelli con cui vogliono effettuare transazioni.
Invece, gli utenti possono inoltrare i pagamenti attraverso connessioni comuni pagando una piccola tassa. Questo processo di instradamento chiamato Routing delle transazioni è una delle funzioni principali di un nodo Lightning.

Lightning Invoice

Livello: intermedio

Argomento: tecnologia

Una Lightning Invoice è simile a una fattura o meglio una richiesta di pagamento, che viene emessa per la rete Lightning Network dal destinatario o beneficiario.

Una Lightning invoice contiene tutte le informazioni di cui il pagante ha bisogno per eseguire correttamente il pagamento: l'importo da pagare, la destinazione del pagamento, i metadati e un messaggio.

Le invoice possono essere considerate l'equivalente Lightning di un indirizzo bitcoin in quanto entrambe vengono inviate dal beneficiario al pagatore per facilitare un pagamento, anche se funzionamento e caratteristiche sono molto diverse. Le Lightning invoice sono generalmente rappresentate come una stringa alfanumerica o a causa della sua lunghezza, sotto forma di codice QR.

Le Lightning invoice sono definite dallo standard BOLT 11. BOLT sta per "Basis of Lightning Technology" e copre tutte le specifiche della rete Lightning. Le specifiche BOLT sono necessarie per consentire a implementazioni separate di funzionare e interagire sulla stessa rete. Pertanto, grazie alle specifiche, una Lightning invoice creata da qualsiasi client o strumento sarà compresa da tutte le altre implementazioni.

URI Scheme: le Lightning invoice possono avere il prefisso `lightning:` per segnalare nei collegamenti 'ipertestuali quale software può essere utilizzato per pagare l'invoice. Idealmente, a lungo termine, con questo schema URI, se si segue un link Lightning sul web, il browser o il sistema operativo indirizzerà l'utente al wallet Lightning di sua scelta dove potrà confermare il pagamento dell'invoice.

La Lightning invoice è costituita da una parte leggibile dall'uomo e da una parte di dati.

Le Lightning invoice, come altre stringhe codificate in Bech32, sono in genere interamente minuscole. Tuttavia, la codifica dei soli caratteri maiuscoli nei codici QR offre notevoli miglioramenti in termini di spazio, motivo per cui le Lightning invoice in maiuscolo sono più frequenti. Questo è anche il motivo per cui un codice QR di una Lightning invoice potrebbe essere decodificato come solo maiuscolo.

Prefisso: una Lightning invoice inizia con le lettere `ln` che stanno per *Lightning Network*.

Network: segue il codice di due lettere che indica quale rete, come definito da BIP 173 per gli indirizzi Segwit nativi:

- **bc** per Bitcoin mainnet
- **tb** per Testnet Bitcoin

- **bs** per Bitcoin signet
- **bcrt** per Bitcoin regtest.

Poiché la invoice è codificata in Bech32, dovrà anche includere il checksum appropriato alla fine.

Importo: il prefisso è seguito dall'importo. Sebbene una tipica Lightning invoice includa un importo, è possibile emettere invoice senza importi. Le invoice Lightning fanno riferimento ai bitcoin, non ai satoshi. Per risparmiare spazio nelle invoice a cifra tonda, l'importo può essere seguito da un moltiplicatore. Una fattura Lightning da un solo satoshi, ad esempio, appare come 10n, cento satoshi come 1u e un milli-satoshi come 10p.

unità	moltiplicatore	satoshi
m (milli)	0.001	100,000
u (micro)	0.000001	100
n (nano)	0.000000001	0.1
p (pico)	0.000000000001	0.0001

Il prefisso e l'importo insieme sono leggibili dall'uomo, consentendo a un utente esperto di identificarla immediatamente come una Lightning invoice e di dedurne l'importo.

Timestamp: la prima parte dei dati è un timestamp unix.

Esiste una serie di tag che possono essere utilizzati per indicare dati aggiuntivi. Alcuni di questi dati sono obbligatori, mentre altri possono essere forniti facoltativamente dal beneficiario.

Attualmente sono definiti i seguenti campi:

- **p** (1): il payment_hash SHA256 a 256 bit, l'hash della preimage del pagamento. Questa preimage viene rivelata successivamente durante il processo di pagamento e può fungere da prova di pagamento.
- **s** (16): Un secret a 256 bit impedisce ai nodi di inoltro di sondare il destinatario del pagamento.
- **d** (13): Descrizione, è possibile aggiungere qui una breve descrizione dello scopo del pagamento, codificata con UTF-8, ad esempio "1 tazza di caffè". Se questo campo non è impostato, deve essere utilizzato al suo posto il tag h.
- **n** (19): La chiave pubblica a 33 byte del nodo del beneficiario può essere inserita qui.
- **h** (23): Se il campo **d** non offre spazio sufficiente, si può includere un hash della descrizione più lunga. Il modo in cui la descrizione completa viene comunicata non è qui definito.
- **x** (6): expiry time, il tempo di scadenza in secondi.

- **c** (24): Il valore min_final_cltv_expiry per l'ultimo HTLC della route. In genere è predefinito a 18.
- **f** (9): Backup Bitcoin Address, è possibile includere un indirizzo on-chain fallback, di ripiego, nel caso in cui il pagamento Lightning non riesca per qualsiasi motivo.
- **r** (3): Una o più voci contenenti informazioni di routing aggiuntive per un routing privato. Questi suggerimenti di instradamento includono:
  - **pubkey** (264 bits)
  - **short_channel_id** (64 bits)
  - **fee_base_msat** (32 bits, big-endian)
  - **fee_proportional_millionths** (32 bits, big-endian)
  - **cltv_expiry_delta** (16 bits, big-endian)
- **9** (5): Uno o più valori a 5 bit contenenti le caratteristiche supportate o richieste per ricevere questo pagamento.

Signature: Infine, l'invoice include una firma. Questa firma viene verificata utilizzando la chiave pubblica fornita nell'invoice.

È possibile decodificare una Lightning invoice per ispezionarne il contenuto con il comando

```
lncli decodepayreq
```

Il formato della Lightning Invoice soffre di alcuni problemi: integrità della firma, mancanza di associazione per utente, mancanza di estrazione dei campi. Inoltre, richiede al destinatario un endpoint statico, come un sito web per comunicare l'invoice. La dipendenza da un sito web introduce una violazione della riservatezza del pagamento, poiché vengono coinvolti i server DNS, e una dipendenza sulla sicurezza della PKI, l'infrastruttura a chiave pubblica del web per la certificazione del sito web.

Attraverso la proposta BOLT 12 vengono aggiunte alle Lightning invoice numerose funzionalità, un nuovo protocollo di richieste di pagamento che introduce le offer.

Lightning Network

Livello: base

Argomento: tecnologia

Lightning Network è una soluzione di livello 2, un second layer, che si trova sopra Bitcoin, consentendo transazioni off-chain più rapide ed economiche.

È un protocollo progettato per aumentare notevolmente la velocità dei tempi di elaborazione delle transazioni in una rete blockchain, spostando off-chain il dettaglio delle transazioni.

Lightning Network è una rete decentralizzata che utilizza la funzionalità smart

contract della blockchain di Bitcoin per consentire pagamenti istantanei attraverso una rete di partecipanti.

Lightning Network può consentire oltre 1 milione di transazioni al secondo, rispetto alle circa 7 transazioni al secondo che può gestire la rete Bitcoin.

L'uso normale di Lightning Network si basa su una tecnologia chiamata canali di pagamento, che vengono aperti tra i nodi.

Il canale è costantemente connesso alla blockchain, motivo per cui i bitcoin sulla blockchain di Bitcoin e i bitcoin sulla rete Lightning sono gli stessi. Non c'è differenza nel valore, è la stessa unità, non un altro token o risorsa.

A grandi linee, il ciclo di vita di un canale consiste in:

- Funding Transaction: è la transazione on-chain di apertura del canale, che dota il canale di liquidità bloccando i bitcoin nella blockchain, e spostandoli virtualmente nel canale;
- Commitment Transaction: sono le transazioni off-chain provvisorie che spostano la liquidità all'interno del canale, e non vengono trasmesse singolarmente nella blockchain;
- Closing Transaction: la transazione di chiusura che gestisce i diversi casi di chiusura collaborativa, forzata o di difesa dal furto con transazioni di revoca.

Un canale di pagamento a due parti viene creato quando entrambe le parti creano una transazione multi-firma 2 su 2 sulla blockchain, con almeno una parte che impegna i fondi nella voce del ledger 2 su 2. Ogni persona ha una chiave privata e le transazioni che spendono dalla voce del ledger possono essere effettuate solo se entrambe le chiavi firmano. Questa transazione iniziale per aprire un canale richiede i soliti tempi di conferma on-chain, ma in seguito i partecipanti possono effettuare transazioni istantanee utilizzando i fondi allocati nel canale. Queste transazioni istantanee avvengono tramite il passaggio di transazioni firmate avanti e indietro, spendendo dalla voce del ledger 2 di 2. Ogni transazione è valida se trasmessa a tutti i canali di pagamento.

Ogni transazione sarebbe valida se trasmessa alla rete e inserita nella blockchain dai minatori della rete, ma in un canale di pagamento le transazioni firmate non vengono trasmesse finché i partecipanti non vogliono che il canale cessi di funzionare. Le transazioni firmate ma non trasmesse vengono scambiate utilizzando una comunicazione diretta peer-to-peer e vengono conservate come ricevute riscattabili dai partecipanti.

Quando viene effettuato un pagamento Lightning, non c'è garanzia che venga effettuato con successo. Ci sono diverse ragioni tecniche per cui i pagamenti possono fallire, come l'impossibilità per i nodi di trovare un percorso efficace perché non ce ne sono di disponibili in quel momento, o il fatto che impieghino troppo tempo a trovare un percorso e vadano in time out dopo un minuto. Nella comunità degli sviluppatori di Lightning sono in corso numerosi sforzi ingegneristici volti a migliorare questi problemi.

I fondi non vengono persi quando i pagamenti non vanno a buon fine, ma questo crea una brutta esperienza utente.

Lightning Network si basa in ultima analisi sulla blockchain sottostante, sia essa di Bitcoin o di altro tipo, per la sua sicurezza. Nel caso di Bitcoin, utilizza l'algoritmo proof-of-work sottostante che protegge l'intera rete per proteggere anche quest'ultima. La blockchain è l'arbitro finale, o in effetti un giudice automatico. Con Lightning, si sa sempre come deciderà il giudice, perché è pre-scritto nelle transazioni utilizzate per creare i canali di pagamento che compongono la rete Lightning. Si tratta di un giudice che non può essere ingannato o corrotto. In effetti, Lightning consente uno stato di "consenso locale", che in ultima analisi viene fatto rispettare dal "consenso globale" (la blockchain). Questo stato di consenso locale non ha una fiducia custodial simile a quella dei modelli tradizionali, in quanto ogni partecipante può chiudere unilateralmente e riscattare i propri fondi senza la cooperazione degli altri partecipanti. In definitiva, Lightning utilizza la blockchain sottostante come mezzo per regolare in batch le transazioni avvenute fuori dalla catena senza la fiducia della controparte.

lightweight client

Livello: intermedio

Argomento: tecnologia

Un client Lightweight, leggeralmente un client Leggero, è u client che non ha una sua blockchain, e deve affidarsi ad un nodo apposito per poter gestire le transazioni.

Invece di fare affidamento sulla tecnologia SPV, che ha implicazioni sulla privacy, si può collegare ad nodo Bitcoin indicato dall'utente, o ad un servizio analogo ad esempio un server Electrum (quali ElectrumX, Electrs, Electrs-Esplora, EPS, BWT).

Un server Electrum mantiene un indice completo di tutte le transazioni Bitcoin per fornire al client Lightweight un avvio istantaneo e una cronologia immediata delle transazioni.

Liquid Network

Livello: avanzato

Argomento: tecnologia

Liquid Network è una sidechain di Bitcoin che consente l'emissione di token di sicurezza e altri asset digitali.
Creata da Blockstream, sul proprio sito viene definita layer-2, anche se tale definizione per alcuni non è appropriata.

Esegue trustless swap utilizzando orderbook non-custodial e protegge la privacy finanziaria degli utenti attraverso confidential transaction, transazioni riservate.

Liquid è una rete di settlement (regolamento) basata su sidechain di Bitcoin che collega exchange di criptovalute e istituzioni in tutto il mondo, consentendo transazioni Bitcoin più veloci e confidenziali e l'emissione di asset digitali. Liquid è un'implementazione di Elements, una piattaforma blockchain open source in grado di gestire le sidechain, basata sul codice di Bitcoin.

Liquid fornisce agli exchange di Bitcoin e agli operatori una serie di potenti funzionalità:

- **Regolamenti veloci e definitivi**: Bitcoin trasferiti alla sidechain di Liquid (Liquid Bitcoin, "L-BTC") possono raggiungere un regolamento definitivo entro due minuti.
- **Transazioni confidenziali**: Importi e tipo di asset trasferiti sono nascosti per impostazione predefinita su Liquid, mantenendo al sicuro i dati finanziari degli utenti.
- **Tokenizzazione sicura**: Nuovi token possono essere emessi sulla sidechain di Liquid (Issued Assets) per rappresentare valute fiat, titoli o altri asset digitali.
- **Interoperabilità**: Una singola integrazione di Liquid fornisce supporto sia per L-BTC che per Issued Assets. Tutti i token si basano sullo stesso standard, consentendo agli utenti di sfruttare funzionalità come scambi atomici e multisig in stile Bitcoin.

Liquid è costruita utilizzando il codice sorgente open source di Elements. È per questo che è possibile scaricare l'applicazione dal repository di Elements, eseguire comandi su elementsd (daemon) ed elements-cli (client) e modificare cose come il file di configurazione elements.conf.

Liquid è una sidechain di Bitcoin che consente agli utenti della Liquid Network di spostare Bitcoin tra le due reti con un peg bidirezionale. Il Bitcoin utilizzato nella Liquid Network è chiamato L-BTC, e ogni L-BTC ha una quantità equivalentemente verificabile di BTC.

Una sidechain è un meccanismo che consente ai token di una blockchain di essere utilizzati in modo sicuro in una blockchain indipendente che funziona in parallelo e utilizza un diverso set di regole, requisiti di prestazioni e meccanismi di sicurezza. Su una sidechain, è possibile spostare i token nuovamente sulla catena originale attraverso un peg bidirezionale. Le sidechain consentono nuove funzionalità che possono comportare compromessi sulla sicurezza o servire come modo per testare nuove caratteristiche che potrebbero non essere pronte per l'uso sulla blockchain principale.

Diversamente da Bitcoin, che per confermare i blocchi che contengono le transazioni si affida ai miner e alla Proof of work, su Liquid tale attività è garantita dai functionaries, in italiano funzionari.
I functionaries sono membri delle federazioni Liquid. Essi sono responsabili

della generazione e della firma di blocchi sulla sidechain. I functionaries partecipano a un processo federato per raggiungere un consenso sulla validità delle transazioni e sulla creazione di nuovi blocchi.

Peg-in (da Bitcoin a Liquid) Il trasferimento di fondi da Bitcoin a Liquid è chiamato peg-in; un utente Liquid invia bitcoin a un indirizzo generato dal software del client Liquid e quindi crea una transazione peg-in per riscattare il suo equivalente Liquid Bitcoin (L-BTC) dalla Liquid Network.

Una transazione peg-in richiede 102 conferme sulla rete Bitcoin prima che i fondi possano essere riscattati sulla Liquid Network. Questo alto livello di sicurezza è necessario per proteggere i fondi di tutti i partecipanti in caso di una grande riorganizzazione dei blocchi della blockchain Bitcoin.

Peg-out (da Liquid a Bitcoin) Il processo di peg-out sposta i fondi da Liquid alla blockchain Bitcoin. Queste transazioni vengono elaborate dai watchmen (guardiani) in batch, dove ogni round di peg-out richiede un tempo di esecuzione previsto di circa 17 minuti.
Il processo di peg-out è non deterministico con un tempo di elaborazione previsto compreso tra 11 e 35 minuti a seconda delle condizioni di rete, come lo stato del guardiano quando è stata avviata la richiesta di peg-out e il numero di altre richieste di peg-out in sospeso da elaborare.

Per una maggiore sicurezza, i watchmen (guardiani) invieranno bitcoin solo a un indirizzo controllato da un utente autorizzato. Questo viene fatto utilizzando una chiave di autorizzazione peg-out (Peg-out Authorization Key, PAK). I Funzionari controllano un elenco di PAK che può essere aggiornato durante l'operazione di rete per determinare quali utenti sono autorizzati a eseguire una transazione di peg-out. Per proteggere Liquid da prelievi non autorizzati, sono necessari tre giorni per aggiornare l'elenco PAK. Ciò consente alla rete di rilevare un attaccore in grado di compromettere un set di Funzionari prima che l'attaccante possa effettuare un prelievo sul proprio portafoglio. Gli ingressi PAK sono collegati a un portafoglio BIP32 Hierarchical Deterministic di proprietà dell'utente. Gli utenti Liquid creano una transazione di peg-out provando che il loro indirizzo è derivato da uno degli ingressi PAK senza rivelare alcuna informazione identificativa aggiuntiva.

Liquid Network AMP

Acronimo di: Asset Management Platform

Livello: avanzato

Argomento: tecnologia

Blockstream AMP è una piattaforma di gestione degli asset che consente agli utenti di emettere e gestire asset con restrizioni di trasferimento o asset tracciati dall'emittente su Liquid Network.

Blockstream AMP è disponibile sotto forma di API, consentendo l'integrazione nei sistemi esistenti e fornendo un modo semplice per esporre gli utenti finali alle funzionalità degli asset di Liquid Network.

Liquidity

Liquidità

Livello: intermedio

Argomento: economia

la liquidità si riferisce alla capacità di scambiare un asset senza modificare sostanzialmente il suo prezzo nel processo e alla facilità con cui un'attività può essere convertita in denaro. Più è facile convertire l'attività in denaro, più l'attività è liquida. Per quanto riguarda i mercati, la liquidità si riferisce alla quantità di attività di negoziazione in un mercato. Maggiore è il volume degli scambi sul mercato, più liquido è il mercato. I mercati liquidi tendono ad aumentare la liquidità delle attività.

La liquidità è un aspetto cruciale del mercato delle criptovalute e ha un impatto determinante, dall'efficacia del trading alla stabilità del mercato. In sostanza, si riferisce alla facilità con cui un asset può essere acquistato o venduto senza influenzare significativamente il suo prezzo. In altre parole, è una misura dell'interesse all'acquisto e alla vendita in un mercato.

Un'elevata liquidità indica un gran numero di partecipanti e un trading attivo, che porta a transazioni più fluide e a una minore volatilità dei prezzi.
Al contrario, una bassa liquidità implica un minor numero di partecipanti e una minore attività di trading, che può comportare una maggiore volatilità dei prezzi e difficoltà di trading.

Il rischio di liquidità, un altro fattore importante da considerare, si riferisce alla possibilità che il mercato diventi rapidamente illiquido, rendendo difficile per i trader uscire dalle loro posizioni. Questo rischio è prevalente in tutti i mercati ed è un fattore critico che i trader esperti considerano nelle loro operazioni. Pertanto, comprendere e prestare attenzione alla liquidità è essenziale per un trading di successo nel mercato delle criptovalute.

Sono diversi i fattori che influenzano la liquidità nel mercato delle criptovalute. Uno dei determinanti chiave è il numero di partecipanti al mercato. Un numero elevato di trader attivi aumenta l'offerta e la domanda dell'asset, migliorando così la liquidità. Inoltre, anche il volume di trading di un asset svolge un ruolo significativo. Gli asset con elevati volumi di trading sono in genere più liquidi, poiché possono essere acquistati o venduti in grandi quantità senza causare movimenti di prezzo significativi. Al contrario, gli asset con bassi volumi di trading sono spesso meno liquidi, rendendo difficile eseguire grandi scambi senza causare fluttuazioni di prezzo.

Un altro fattore critico è la disponibilità e l'accessibilità dell'asset su vari exchange. Le criptovalute quotate su più exchange e facilmente accessibili ai trader tendono ad avere una liquidità maggiore. Al contrario, le criptovalute difficili da accedere o quotate su meno exchange hanno in genere una liquidità inferiore.

Inoltre, le condizioni di mercato e i fattori economici possono influenzare anche la liquidità. Ad esempio, durante periodi di incertezza del mercato o di crisi economiche, la liquidità può prosciugarsi rapidamente, poiché i trader diventano riluttanti ad acquistare o vendere.

Nel mondo del trading di criptovalute, la liquidità gioca un ruolo fondamentale nel mantenimento della stabilità dei prezzi. Un'elevata liquidità in un mercato significa che c'è un volume di trading sostanziale, che si traduce in fluttuazioni di prezzo più ridotte. Ciò è dovuto al fatto che un mercato altamente liquido ha molti partecipanti, il che garantisce che ci sia sempre qualcuno disposto ad acquistare o vendere un asset, mantenendo così i prezzi stabili. Ad esempio, una criptovaluta con un'elevata liquidità come Bitcoin avrà un prezzo relativamente stabile, poiché grandi quantità possono essere acquistate o vendute senza influenzare significativamente il suo prezzo.

D'altra parte, una criptovaluta con bassa liquidità può subire drastiche variazioni di prezzo anche con piccoli scambi. Ciò è dovuto al fatto che ci sono meno partecipanti al mercato, il che rende difficile trovare un acquirente o un venditore al prezzo desiderato.

Inoltre, un'elevata liquidità protegge il mercato anche dalla manipolazione dei prezzi. In un mercato con bassa liquidità, un singolo scambio significativo può alterare drasticamente il prezzo dell'asset, aprendo la strada a potenziali manipolazioni dei prezzi. Pertanto, per mantenere la stabilità dei prezzi e un ambiente di trading equo, la liquidità è un fattore fondamentale nel mercato delle criptovalute.

Nel contesto dei mercati delle criptovalute, i fornitori di liquidità svolgono un ruolo essenziale nel facilitare transazioni fluide e nel mantenere la stabilità del mercato. I fornitori di liquidità sono partecipanti al mercato, spesso grandi istituzioni finanziarie o aziende, che forniscono ordini di acquisto e vendita per migliorare la liquidità del mercato. Assicurano che ci sia sempre una scorta di un asset disponibile per il trading, consentendo così ai trader di eseguire le loro transazioni rapidamente senza influenzare significativamente il prezzo dell'asset.

Senza i fornitori di liquidità, il mercato potrebbe diventare illiquido, con ampi spread bid-ask e fluttuazioni di prezzo sostanziali

Liquidità su Lightning Network Nel contesto di Lightning Network, la liquidità si riferisce alla capacità di spostare fondi tra i partecipanti alla rete. Definire e gestire correttamente la liquidità può essere complesso su Lightning Network, ma questa complessità è ricompensata dalla maggiore fluidità dei movimenti di valore rispetto ad altri sistemi o reti.

La liquidità di un canale lightning è l'ammontare di Bitcoin impegnati (committed) a quel canale, e può essere distinta in:

- Inbound Liquidity, o liquidità in entrata, la capacità di ricevere bitcoin
- Outbound Liquidity, o Liquidità in uscita, la quantità di bitcoin che può essere inviata

La liquidità di bitcoin on-chain è probabilmente la più facile da capire. Una transazione bitcoin on-chain può essere spostata in qualsiasi momento a fronte di una commissione prevedibile, ma variabile. Questa fee proposta non garantisce l'inclusione in un blocco, ma rappresenta piuttosto un'offerta in un processo d'asta perpetuo in cui i miner scelgono dalla mempool le transazioni che pagano la tariffa più alta. Queste vengono incluse in un blocco, che viene creato in media ogni 10 minuti. Alcune transazioni on-chain, come le chiusure unilaterali dei canali (chiamate anche force closes), hanno proprietà di liquidità uniche. In genere, la parte che avvia la chiusura forzata deve aspettare per spendere i propri bitcoin, mentre l'altra parte può spendere i propri fondi immediatamente. La durata del periodo di attesa viene definita al momento dell'apertura del canale. Può variare da un solo giorno a qualche settimana. Queste chiusure forzate possono essere l'unico modo per recuperare fondi da un canale "illiquido" se un peer non è online da un po'. Possono anche essere richieste dal peer in caso di perdita di dati o possono essere il risultato di un HTLC che deve essere regolato on-chain.

Liquidity pool

Livello: intermedio

Argomento: finanza

Una liquidity pool (o "pool di liquidità" in italiano) è un meccanismo utilizzato nelle piattaforme di trading decentralizzate DEX basate sulla tecnologia blockchain.
In una liquidity pool i Liquidity provider, fornitori di liquidità, depositano coppie di token in una riserva, che viene utilizzata per facilitare gli scambi tra i token nella coppia. Ad esempio, se si vuole scambiare il token A con il token B, la liquidity pool deve avere una riserva di entrambi i token.
In cambio del loro deposito, i Liquidity provider ricevono dei token rappresentativi della loro quota nella pool, noti come LP token. Questi LP token rappresentano la partecipazione del fornitore di liquidità nella pool e possono essere scambiati come qualsiasi altro token.

Le liquidity pool sono asset crittografici che vengono utilizzati per facilitare lo scambio di coppie di trading su exchange decentralizzati. Tramite le liquidity pool i client non fanno trading su un portafoglio ordini presso un exchange, ma direttamente con altri partecipanti al pool, che hanno già depositato nel pool i fondi che si trovano su smart contract.

Gli utenti possono quindi scambiare i loro token nella coppia nella liquidity pool,

utilizzando il prezzo determinato dall'algoritmo della pool. Il prezzo è calcolato in base alla proporzione di ciascun token presente nella riserva della pool.
Il vantaggio di utilizzare una liquidity pool è che i prezzi delle coppie di token sono determinati dal mercato stesso e non dalle istituzioni finanziarie centralizzate. Inoltre, i Liquidity provider guadagnano una quota degli scambi effettuati sulla pool, sotto forma di commissioni.

Le liquidity pool sono anche il nome dato all'incrocio degli ordini che creano livelli di prezzo che, una volta raggiunti, vedono l'asset decidere se continuare a muoversi in tendenza al rialzo o al ribasso. Gli exchange decentralizzati che utilizzano le liquidity pool sono gli stessi che utilizzano sistemi basati su market maker automatizzati. Su tali piattaforme di trading, il tradizionale order book è sostituito da pool di liquidità prefinanziate on-chain per entrambi gli asset della coppia di trading. Il vantaggio dell'utilizzo delle liquidity pool è che non richiede un acquirente e un venditore che decidano di scambiare due asset per un dato prezzo, ma utilizza invece una liquidity pool prefinanziata. Ciò consente che gli scambi avvengano con una slippage limitata anche per le coppie di trading più illiquide, purché esista una liquidity pool abbastanza grande.

I fondi detenuti nelle liquidity pool sono forniti da altri utenti che guadagnano anche un reddito passivo sul loro deposito attraverso commissioni di trading basate sulla percentuale di liquidity pool che forniscono.

Uno dei primi exchange decentralizzati a introdurre tale sistema è stato il sistema di trading basato su Ethereum Bancor, ma è stato ampiamente adottato nello spazio dopo che Uniswap li ha resi popolari.

Liquidity provider

Fornitore di liquidità

Livello: avanzato

Argomento: finanza

Un liquidity provider è un fornitore di liquidità che alimenta un liquidity pool con asset cripto che possiede, al fine di agevolare il trading sulla piattaforma e guadagnare un reddito passivo sul suo deposito.

I liquidity pool sono utilizzati dai dex che utilizzano sistemi automatizzati basati su market maker per consentire il trading di coppie di scambio illiquide con slippage limitato.
Invece di utilizzare i tradizionali sistemi di negoziazione basati sull'order book, tali scambi utilizzano i fondi detenuti per ogni asset in ogni coppia di negoziazione per agevolare l'esecuzione degli scambi.

Mentre il trading di coppie di trading illiquide su exchange basati su order book potrebbe portare a soffrire di un grande slippage e l'impossibilità di eseguire gli scambi, il vantaggio dei liquidity provider è che gli scambi possono sempre essere eseguiti finché i liquidity pool sono sufficientemente grandi. Per questo

motivo, i liquidity provider sono visti come facilitatori di scambi e pagati con le commissioni di transazione pagate per gli scambi che hanno attivato.

Quanto vengono pagati i liquidity provider si basa sulla percentuale del pool di liquidità che forniscono. Quando finanziano il pool, di solito sono tenuti a finanziare due diversi asset per consentire ai trader di passare da uno all'altro scambiandoli in coppia.

Un liquidity provider è un soggetto che fornisce liquidità a un mercato finanziario. In altre parole, un liquidity provider è un soggetto che compra e vende strumenti finanziari per conto proprio o per conto di terzi nel tentativo di mantenere il mercato in movimento. I Liquidity Provider agiscono come market maker, assicurando che ci siano sempre abbastanza fondi disponibili per gli investitori che vogliono acquistare o vendere un bene.

litecoin

Livello: base

Argomento: tecnologia

Litecoin è una criptovaluta p2p open source creata nel 2011 da Charlie Lee, un ex ingegnere di Google.

Il codice di Litecoin è derivato da quello di Bitcoin, al quale sono state apportate alcune modifiche, ad esempio sul tempo di blocco più breve (2,5 minuti contro i 10 minuti di Bitcoin) e nel limite di emissione di 84 milioni di monete (contro i 21 milioni di Bitcoin).

Litecoin è stato anche utilizzato per testare su una moneta reale oltre che nella testnet alcune implementazioni prima di essere applicate su Bitcoin.
Eccone alcune:

- 12 gennaio 2017 client SegWit rilasciato nella versione 0.13.2.1
- maggio 2017 SegWit attivato il softfork
- 10 maggio 2017 Lightning Network: Christian Decker, un developer Bitcoin e Core Tech Engineer a Blockstream, ha fatto la prima transazione Lightning Network utilizzando la mainnet Litecoin

LN Routing

Acronimo di: Lightning Network Routing

Livello: avanzato

Argomento: tecnologia

Il routing su Lightning Network è il processo attraverso il quale i pagamenti vengono instradati attraverso la rete, dai nodi mittenti ai destinatari attraverso i canali Lightning Network tra i nodi. In sostanza, il routing è il modo in cui

i pagamenti vengono smistati tra i vari nodi intermedi che compongono la rete di Lightning.

Quando un utente invia un pagamento su Lightning Network, il pagamento composto in smart contract chiamati HTLC (Hashed Time-Locked Contract), che vengono poi instradati attraverso i nodi intermedi componendo un percorso dal mittente al destinatario. Ogni nodo intermedio nella catena di routing può scegliere di inoltrare il pagamento o meno, a seconda della propria politica di routing, della liquidità e della disponibilità di canali aperti.

Per instradare i pagamenti attraverso la rete di Lightning, ogni nodo deve conoscere i canali aperti e le capacità di pagamento dei nodi vicini, così da poter scegliere il percorso più breve e conveniente per il pagamento in un processo chiamato pathfinding.

In generale, il routing su Lightning Network è un aspetto critico del funzionamento della rete, poiché determina la capacità della rete di instradare i pagamenti in modo efficiente e affidabile.

LNP/BP

Acronimo di: Lightning Network Protocol / Bitcoin Protocol

Protocollo della rete Lightning / Protocollo Bitcoin

Livello: avanzato

Argomento: politica

LNP/BP è l'acronimo di Lightning Network Protocol / Bitcoin Protocol.

Viene usata per identificare il protocollo Lightning Network, e più precisamente per indicare oltre a Lightning Network anche il protocollo Bitcoin e stabilire tra questi una forte correlazione, se non addirittura voler suggerire una interdipendenza reciproca.

In alternativa a LNP/BP, viene spesso utilizzata la sigla BTC/LN con significato analogo.

Entrambe le sigle hanno un formato che richiama la suite di protocolli alla base di Internet, nota come TCP/IP, con il possibile scopo di creare un parallelismo tra Bitcoin e Internet, e l'architettura a layer dove il protocollo Bitcoin si trova al layer 1, e quello Lightning Network al layer 2.

LNURL

Livello: avanzato

Argomento: tecnologia

In genere, quando un utente desidera ricevere un pagamento su Lightning Network, deve generare un invoice.

LNURL è uno standard che consente di ricevere satoshi su Lightning senza che l'utente debba fornire un invoice.

LNURL elimina questa complessità consentendo di creare un codice QR statico riutilizzabile o un link URL statico che si può utilizzare per pagare un altro utente Lightning.

LNURL è uno stack di semplici protocolli per coordinare le informazioni necessarie per effettuare pagamenti tramite Lightning Network utilizzando HTTP.

LNURL ha smussato e migliorato gran parte dell'esperienza utente sull'utilizzo di Lightning Network, ma richiede l'uso di un server Web per essere utilizzato. Tutte le richieste e le risposte vengono gestite tramite HTTP e per gestire queste modalità semplificate di coordinamento ed esecuzione dei pagamenti è necessaria un'infrastruttura aggiuntiva oltre al nodo Lightning stesso. Questo è un requisito perfettamente ragionevole per qualsiasi fornitore di servizi online o commerciante, che realisticamente avrà comunque bisogno di un server Web per fornire i propri servizi o prodotti online.

Tuttavia, per un utente finale non tecnico che da casa desidera semplicemente un'esperienza più semplice, un venditore ambulante, un negozio fisico o altri utenti che non hanno a disposizione un server web, questo può essere un requisito pesante e potenzialmente rischioso

Tre elementi fondamentali del protocollo LNURL sono:

- uno schema di autenticazione, in cui una chiave pubblica può essere utilizzata per accedere a un servizio
- uno schema di invoice, o richiesta di pagamento, con il quale un wallet può eseguire il ping di un server tramite un codice QR statico e recuperare una invoice
- uno schema di richiesta di prelievo (withdraw request) con il quale un wallet può eseguire il ping di un server e richiedere che il server paghi una fattura fornita dal wallet.

Le invoice lightning sono molto più lunghe degli indirizzi Bitcoin on-chain, il pagamento stesso è un processo interattivo che richiede a entrambe le parti di essere online, quindi ha senso coordinare i dettagli di pagamento in modo interattivo su una connessione di rete.

Il protocollo di autenticazione è di fatto solamente il server che fornisce un numero generato casualmente che il wallet dell'utente firma con una chiave appena generata. Dopo che il valore casuale firmato è stato ricevuto dal server, salva la chiave associata da utilizzare negli accessi futuri.

locking script

Livello: avanzato

Argomento: tecnologia

Uno locking script, script di blocco, è una condizione di spesa impostata su un'output: specifica le condizioni che devono essere soddisfatte per spendere l'output in futuro. Storicamente, il locking script era chiamato scriptPubKey, perché di solito conteneva una chiave pubblica o un indirizzo Bitcoin (hash della chiave pubblica).

Il termine locking script potrebbe essere più adatto perché aiuta a comprendere la gamma molto più ampia di possibilità di questa tecnologia di scripting.

Nella maggior parte delle applicazioni bitcoin, quello che chiamiamo locking script apparirà nel codice sorgente come scriptPubKey.

Il locking script viene anche chiamato witness script (vedi segwit) o più in generale puzzle crittografico.

Questi termini significano tutti la stessa cosa, a diversi livelli di astrazione.

Per sbloccare il locking script e quindi poter spendere l'UTXO su cui è impostato, è necessario eseguire lo script di sblocco o unlocking script corrispondente per vedere se soddisfa la condizione di spesa.

Il fatto che le transazioni siano bloccate con gli script significa che possono essere bloccate in una varietà di modi diversi, richiedendo una varietà di chiavi diverse. Per ottenere meccanismi di blocco diversi, vengono utilizzati degli opcode diversi, ad esempio:

- OP_CHECKSIG, che verifica una chiave pubblica rispetto a una firma, è la base del classico indirizzo P2PKH
- OP_CHECKMULTISIG controlla in modo analogo i multisig
- OP_CHECKLOCKTIMEVERIFY o CLTV e OP_SEQUENCEVERIFY o CSV costituiscono la base di timelock più complessi
- OP_RETURN che consente una transazione non spendibile, che viene di solito utilizzato per trasportare dati

Long

Livello: intermedio

Argomento: finanza

Una situazione in cui si acquista una criptovaluta con l'aspettativa di venderla a un prezzo più alto per profitto dopo un lungo periodo di tempo, non facendo trading giornaliero.

Long Position

Livello: intermedio

Argomento: finanza

Una posizione long significa che un investitore ha un'esposizione positiva su un certo titolo. Andare long (noto anche come "longing") è un processo di investimento in base al quale un investitore acquista una criptovaluta, un titolo, un derivato o un altro tipo di attività che crede aumenterà di valore (soprattutto a lungo termine), invece di andare allo scoperto in cui il l'investitore si aspetta che il prezzo di una specifica attività diminuisca di valore.

Long Squeeze

Livello: avanzato

Argomento: finanza

Un long squeeze si verifica quando un improvviso calo del prezzo di un'azione o di un altro bene incita ad ulteriori vendite. In un long squeeze, i possessori di posizioni long su un titolo sono spinti a venderlo per proteggersi da una perdita drammatica. Un long squeeze si verifica quando la vendita incita ulteriori vendite, alimentando un ciclo e un grande calo del prezzo. I long squeeze sono più comuni nelle attività che hanno visto un aumento drammatico dei prezzi con un volume molto alto che si verifica quando il prezzo si abbassa, e nelle azioni a bassa liquidità o a basso flottante. Gli investitori e i trader di valore che cercano condizioni di ipervenduto, sono in grado di osservare e acquistare titoli long squeeze.

Longest chain

Catena più lunga

Livello: intermedio

Argomento: tecnologia

La catena più lunga, **longest chain** a volte indicata anche come **best chain**, è un elemento del meccanismo di consenso dei bitcoin. Nel white paper Bitcoin di Satoshi Nakamoto si dice:

La catena più lunga serve come prova che essa proviene dal gruppo che ha la più grande potenza CPU. Fintanto che la maggior parte della potenza di calcolo è controllata da nodi che non cooperano per attaccare la rete, questi genereranno la catena più lunga e supereranno gli utenti malintenzionati …

La decisione della maggioranza è rappresentata dalla catena più lunga, su cui è stato speso il massimo sforzo di proof-of-work. Se la maggioranza della potenza di calcolo è controllata da nodi onesti, la catena onesta crescerà più velocemente e supererà eventuali catene concorrenti. …

I nodi considerano sempre come corretta la catena più lunga e continueranno a lavorare per allungarla. Se due nodi trasmettono diverse versioni del blocco successivo contemporaneamente, alcuni nodi possono ricevere l'una o l'altra prima. In tal caso, questi lavorano sul primo che hanno ricevuto, ma salvano l'altra ramificazione nel caso diventi più lunga. Questo impasse sarà risolto quando la proof-of-work successiva viene trovata e una delle ramificazioni diventa più lunga; i nodi che stavano lavorando sull'altra ramificazione a quel punto si sposteranno su quella più lunga.

Inizialmente Satoshi aveva stabilito il consenso sulla catena con il maggior numero di blocchi validi come metrica per determinare la catena più lunga. Però scegliere la catena semplicemente contando i blocchi consente alcuni attacchi estremamente facili da effettuare, e nel 2010 è stato introdotto il calcolo del ChainWork per determinare la catena più lunga.

Il ChainWork è uguale alla somma del BlockWork dei suoi blocchi, ovvero al valore cumulativo della proof of work. Il BlockWork è il numero medio di hash che si prevede siano necessari da calcolare per generare un blocco data una certa difficulty (quindi è diverso dalla difficulty ma dipende da questa). Siccome la difficulty viene regolata ogni 2016 blocchi (circa ogni 2 settimane), i blocchi minati nell'intervallo di tempo nel quale c'è la stessa difficoltà hanno lo stesso BlockWork. Alla BlockWork si è poi sostituita la BlockProof.

LSAT

Acronimo di: Lightning Service Authentication Token

Livello: avanzato

Argomento: tecnologia

LSAT Lightning Service Authentication Token, Token per l'autenticazione ai servizi Lightning, sono dei Macaroon che includono un hash di pagamento.

Affinché un LSAT sia valido, deve essere presentato insieme alla preimage corrispondente all'hash del pagamento.

I token di autenticazione del servizio Lightning (LSAT) sfruttano le capacità dei Macaroon e le caratteristiche programmatiche della rete Lightning per creare un meccanismo che consente ai sistemi distribuiti di autenticare un utente e la ricevuta di pagamento. Questa autenticazione avviene senza richiedere l'accesso a un database centrale di utenti o Invoice.

Le LSAT sono una pietra miliare per la costruzione di API misurate per l'economia machine-to-machine, senza login, indirizzi e-mail o password.

Un LSAT è un Macaroon insieme alla preimage di un pagamento Lightning Network. Il Macaroon viene trasmesso all'utente tramite HTTP insieme a una Invoice Lightning e contiene l'hash del pagamento della Invoice come avviso.

Per essere un LSAT valido, l'utente deve presentare due informazioni:

- Il LSAT parziale, ovvero il Macaroon comprensivo dell'hash di pagamento.
- La preimage, che può essere ottenuta pagando la Invoice Lightning.

Poiché l'hash del pagamento è un hash della preimage e la preimage può essere ottenuta solo pagando interamente la Invoice Lightning, è facile per chiunque abbia la root key verificare che l'LSAT sia stato emesso:

- che l'LSAT sia stata emessa dall'autorità competente
- che l'LSAT sia dotato delle funzionalità pertinenti
- che la Invoice Lightning sia stata pagata

LSP

Acronimo di: Lightning Service Provider

Fornitore di servizi Lightning

Livello: avanzato

Argomento: tecnologia

I canali della rete Lightning hanno delle naturali limitazioni dovute alle loro dimensioni, e la loro capacità è ulteriormente limitata dai balance locali e remoti.

Gli LSP, Lightning Service Provider o fornitori di servizi Lightning Network, aiutano gli utenti a connettersi alla rete lightning mantenendo gli utenti in modalità self-cusotdy e quindi non-custodial.

Lo fanno essendo ben collegati alla rete, aprendo canali e offrendo liquidità in entrata agli utenti. Spesso applicano una tariffa per i loro servizi.

Alcuni LSP possono anche offrire servizi di gestione dei canali, routing (instradamento), backup e altri servizi, ma questi non si limitano a essere offerti dagli LSP.

Per utilizzare Lightning Network, un utente self-custody ha bisogno di almeno un canale di pagamento. Per inviare pagamenti, questo canale ha bisogno di outbound liquidity, liquidità in uscita, che di solito l'utente fornisce. Per ricevere i pagamenti, questo canale ha bisogno di Inbound Liquidity, o liquidità in entrata, che deve essere fornita da qualcun altro.

Trovare qualcuno che offra liquidità in entrata e che gli apra un canale può essere difficile, soprattutto per i nuovi utenti. Gli LSP forniscono liquidità in entrata e aprono canali per gli utenti.

Gli LSP possono modificare le modalità di apertura dei canali per fornire modalità specifiche per gli utenti. Queste possono comportare ulteriori compromessi in termini di fiducia o di privacy, per cui gli utenti devono esserne consapevoli ed essere in grado di rifiutarle se utilizzate.

Un LSP può aprire un canale e offrire all'utente diverse funzionalità:

Collaborative fund o Dual Funding I canali sono solitamente finanziati solo da un lato, il che significa che inizialmente una parte non sarà in grado di inviare e l'altra non sarà in grado di ricevere.

Un Collaborative fund o fondo collaborativo, chiamato anche Dual Funding, consente a entrambe le parti di contribuire con fondi bitcoin al canale. Ciò significa che entrambe le parti possono inviare e ricevere una volta che il canale è aperto.

Liquidità On-demand Se un utente tenta di ricevere un pagamento senza sufficiente liquidità in entrata, il pagamento fallirà.

In queste situazioni, un LSP può risolvere questo problema con liquidità On-demand, aggiunta su richiesta, aprendo un nuovo canale con l'utente, dando all'utente liquidità in entrata sufficiente per ricevere il pagamento.

On-chain funding Un utente può avere solo bitcoin on-chain con cui finanziare il proprio lightning wallet. Un LSP può consentire agli utenti di aprire un canale utilizzando un pagamento on-chain con uno swap.

Gli LSP dovranno fornire sufficiente liquidità in entrata per inoltrare il pagamento all'utente. Spesso forniscono più dell'importo del pagamento inoltrato, in modo che l'utente possa ricevere ulteriori pagamenti con il canale.

Zero-confirmation L'apertura di un canale di pagamento richiede che venga prima effettuata una transazione on-chain che deve essere anche confermata, il che lascia gli utenti in attesa per poter effettuare una spesa nel loro canale.

Un canale a Zero-confirmation consente agli utenti di utilizzare il canale senza che venga confermato on-chain. Questo rende più veloce l'ingresso degli utenti, ma comporta che bisogna riporre fiducia nei confronti dell'LSP che non annullerà la transazione dopo che i pagamenti sono stati effettuati.

Graph e calcolo del routing Tenere aggiornato il grafo dei canali che connettono i vari nodi e calcolare in modo efficiente i percorsi ottimali può essere un esercizio intensivo per i dispositivi con prestazioni limitate. I nodi che fungono da "nodi trampolino" possono gestire questo routing per gli utenti finali in configurazioni che sono trustless e private, una volta che la loro disponibilità sulla rete è sufficientemente diffusa.

Ad esempio wallet come Phoenix utilizzano questa tecnica per la creazione di grafici e l'instradamento.

Backup e ripristino dei canali Gli LSP possono agire come peer fidati che memorizzano un SCB Static Channel Backup crittografato per i propri utenti.

ACINQ (l'LSP) e il suo wallet non-custodial Phoenix utilizzano questo metodo di backup. Nel caso in cui un utente debba ripristinare il proprio wallet, tutto

ciò di cui ha bisogno è la sua normale recovery phrase e i suoi canali con ACINQ saranno recuperati dall'SCB crittografato che ACINQ memorizza in modo affidabile con il suo nodo.

Watchtower Le Watchtower (letteralmente torri di controllo) sono un servizio di sicurezza della rete Lightning che monitorano i canali di pagamento alla ricerca di potenziali violazioni del protocollo. Se uno dei partner del canale va offline o perde il proprio backup, una Watchtower conserva i backup e può ripristinare le informazioni del canale.

I fornitori di servizi Lightning di solito aiutano a gestire la liquidità di un utente svolgendo uno dei due compiti seguenti * scambiare fondi on-chain con fondi off-chain o viceversa * aprire canali per aumentare la capacità in entrata di un utente o migliorare la sua posizione nel grafico

Idealmente, un fornitore di servizi Lightning interagisce con i propri clienti in modo puramente non-custodial. Gli swap possono essere costruiti come Submarine Swap per garantire che il fornitore di servizi non possa appropriarsi dei fondi in nessun momento. Quando apre canali con i peer, l'LSP mantiene la custodia del proprio lato del canale e guadagna le fee di routing (instradamento) quando inoltra i pagamenti.

Gli LSP sono noti soprattutto per fornire liquidità agli utenti di wallet non-custodial sotto forma di canali. In questo modo gli utenti possono ricevere immediatamente i pagamenti lampo nei loro wallet senza dover gestire attivamente il canale o possedere un UTXO. L'LSP in genere richiede un pagamento anticipato per compensare le fee di estrazione e i costi di capitale.

Queste fee sono spesso detratte direttamente da un pagamento in entrata, ma potrebbero anche essere addebitate in anticipo. Può essere difficile per l'LSP valutare quanto debba essere grande un nuovo canale per un utente.

Un LSP può prendere in prestito bitcoin per questo compito o impiegare i propri fondi. È anche possibile che un LSP acquisti tali canali sul mercato aperto, come Lightning Pool che utilizza canali sidecar, invece di aprirli da solo.

macaroons

Livello: avanzato

Argomento: tecnologia

Un macaroon può essere considerato simile ad un cookie.

I cookie sono piccoli frammenti di dati che il browser memorizza e invia a un determinato sito Web quando effettua una richiesta a quel sito Web. Quando si effettuata l'accesso a un sito Web, quel cookie può memorizzare un ID di sessione, che il sito può cercare nel proprio database per verificare chi sei e fornirti il contenuto appropriato.

Un macaroon è simile: è una piccola quantità di dati che un client (come lncli) può inviare a un servizio (come lnd) per dimostrare che gli è consentito eseguire un'azione. Il servizio cerca l'ID macaroon e verifica che l'macaroon sia stato inizialmente firmato con la chiave radice del servizio. Tuttavia, a differenza di un cookie, puoi delegare un macaroon o crearne una versione con capacità più limitate e quindi inviarlo a qualcun altro per utilizzarlo.

I macaroon sono credenziali di autorizzazione che forniscono un supporto flessibile per la condivisione controllata in sistemi decentralizzati e distribuiti come Lightning. Un macaroon può interfacciarsi con i servizi e consentire l'esecuzione di azioni per conto di un nodo Lightning.

Proprio come un cookie, un macaroon dovrebbe essere inviato su un canale sicuro (come una connessione crittografata TLS). Prima che SSL (l'utilizzo del protocollo sicuro https) fosse applicato su siti Web come Facebook e Google, l'ascolto di sessioni HTTP su reti wireless era un modo per dirottare la sessione e accedere come quell'utente, ottenendo l'accesso all'account dell'utente. I macaroon sono simili in quanto l'intercettazione di un macaroon in transito consente all'intercettore di utilizzare l'macaroon per ottenere tutti i privilegi dell'utente legittimo.

Mainnet

Livello: intermedio

Argomento: tecnologia

La mainnet di Bitcoin è la rete principale e ufficiale di Bitcoin. È dove avvengono le transazioni reali con la criptovaluta Bitcoin (BTC) e dove viene mantenuto il registro pubblico e immutabile di tutte le transazioni Bitcoin mai effettuate. Il termine può essere usato anche da altre coin diverse da Bitcoin, per indicare quando un protocollo blockchain è completamente sviluppato, distribuito, e attivo il che significa che le transazioni di criptovaluta vengono trasmesse, verificate e registrate sulla relativa blockchain.

Si contrappone a mainnet il termine testnet.

Maker

Livello: intermedio

Argomento: finanza

Diventi un "maker" quando effettui un ordine e questo non viene scambiato immediatamente, quindi il tuo ordine rimane nell'order book e attende che qualcun altro lo evada/abbini in seguito.

Un ordine maker si verifica quando un trader inserisce un ordine che rimane sull'order book di una borsa per un certo periodo di tempo invece di essere eseguito immediatamente.

Ciò può accadere quando un ordine limite viene inviato a un prezzo che non può essere soddisfatto istantaneamente.
Gli ordini maker creano la liquidità tà su un mercato che consente l'esecuzione degli ordini taker. È prassi comune che le borse offrano commissioni più basse agli ordini del produttore per incentivare i trader ad aggiungere liquidità all'order book.

Margin

Livello: intermedio

Argomento: finanza

Nel Marging Trading, attraverso il quale un investitore può effettuare investimenti per importi superiori alla disponibilità del proprio capitale, si chiama Margin l'importo che l'investitore ha inizialmente e che viene utilizzato come Collaterale.

Margin call

Livello: intermedio

Argomento: finanza

La Margin Call è la richiesta che viene fatta all'investitore da un intermediario, ad esempio un exchange, di coprire le perdite in una operazione di Margin Trading. Quando un investitore acquista e vende titoli utilizzando una combinazione di fondi propri e denaro preso in prestito da un broker, si parla di Margin Trading. Il capitale di un investitore nell'investimento è uguale al valore di mercato dei titoli, meno l'importo dei fondi presi in prestito dal proprio broker.

Viene effettuata una Margin Call quando il capitale dell'investitore, come percentuale del valore di mercato totale dei titoli, diminuisce al di sotto di un determinato requisito percentuale (chiamato margine di mantenimento). Se l'investitore non può permettersi di pagare l'importo necessario per portare il valore del proprio portafoglio fino al margine di mantenimento del conto, il broker potrebbe essere costretto a liquidare i titoli utilizzati come collaterale.

Margin Trading

Livello: intermedio

Argomento: finanza

Avvertenza: se sei un nuovo trader e vuoi provare il margin trading, se utilizzi una leva finanziaria elevata puoi perdere tutto in pochi secondi.

In poche parole, un trader prende in prestito denaro dall'exchange per moltiplicare i propri fondi e usa quel denaro preso in prestito per acquistare coin e rimborsare il prestito.

Fare margin trading significa giocare al gioco più difficile del mondo contro i migliori giocatori che hanno più informazioni di te e più fondi di te. Solo una piccola percentuale di persone fa guadagni con il margin trading, gli altri vengono mangiati vivi.
Il Margin Trading è una forma di speculazione in cui scambi bitcoin usando denaro preso in prestito oltre al tuo (il rapporto tra denaro totale e denaro è la leva), consentendo profitti molto più alti ma rischiando la liquidazione (perdendo tutti i tuoi soldi) se il prezzo diminuisce, ad esempio, del 20 percento con una leva finanziaria di 5 a 1. È anche possibile utilizzare il margin trading per scommettere contro bitcoin (shorting), nel qual caso stai acquistando dollari con bitcoin preso in prestito, quindi guadagni un profitto se il prezzo del bitcoin scende e vieni liquidato se il prezzo del bitcoin aumenta troppo.

Market Cap

Capitalizzazione di mercato

Livello: base

Argomento: economia

Il Market Cap, o Capitalizzazione di mercato, è un indicatore del valore totale di una criptovaluta, ovvero la somma del valore di tutti i coin o token in circolazione.

Viene calcolato moltiplicando il numero di asset, coin o token, esistenti per il prezzo di mercato corrente di tali asset.

Nei mercati finanziari tradizionali, la capitalizzazione di mercato di un'azienda corrisponde al valore di tutte le azioni della società. Viene calcolata moltiplicando il prezzo attuale dell'azione di una società per il numero totale di azioni emesse. Ad esempio, se una società ha emesso 1 milione di azioni e il prezzo attuale degli asset è di $ 50, la capitalizzazione di mercato della società sarà di $ 50 milioni.

La capitalizzazione di mercato viene spesso utilizzata come indicatore della dimensione di una società rispetto ad altre società. Ad esempio, una società con una capitalizzazione di mercato di $ 1 miliardo sarà considerata più grande di una società con una capitalizzazione di mercato di $ 100 milioni.

Tuttavia, la capitalizzazione di mercato non è l'unico fattore che determina il valore di una società e non sempre rappresenta accuratamente il suo valore intrinseco.

Ci sono diverse critiche nei confronti della capitalizzazione di mercato come indicatore del valore di una crypto o società. Ecco alcune delle principali critiche:

- Prezzo degli asset: il prezzo degli asset di una cripto o delle azioni di una società può essere influenzato da molti fattori, come le aspettative degli

investitori, le notizie o le emozioni del mercato. Ciò significa che il prezzo degli asset potrebbe non riflettere accuratamente il suo valore intrinseco.

- Volatilità: il prezzo delle criptovalute può essere altamente volatile, il che significa che il valore di una criptovaluta può variare in modo significativo in un breve periodo di tempo. Ciò può rendere difficile utilizzare la capitalizzazione di mercato come indicatore del valore di una criptovaluta.
- Differenze di prezzo: il prezzo di una criptovaluta può variare significativamente su diversi Exchange. Ciò può rendere difficile calcolare la capitalizzazione di mercato di una criptovaluta in modo accurato, poiché il prezzo di una criptovaluta su un Exchange può essere significativamente diverso da quello su un altro Exchange.
- Mancanza di fondamenta: alcune criptovalute non hanno una base solida di attività o beni sottostanti, il che significa che il loro valore potrebbe essere basato principalmente sulla speculazione. È inoltre molto semplice creare un nuovo token, e immetterlo sul mercato. Ciò può rendere difficile utilizzare la capitalizzazione di mercato come indicatore del valore di una criptovaluta.
- Peso degli asset: alcuni asset hanno un peso maggiore della capitalizzazione di mercato di una società rispetto ad altre. Ad esempio, se una società ha emesso un numero limitato di azioni di proprietà di un solo individuo o di un gruppo di individui, queste azioni potrebbero avere un peso maggiore nella capitalizzazione di mercato della società rispetto ad altre azioni. Ciò significa che la capitalizzazione di mercato potrebbe essere influenzata in modo non equo da tutte le azioni emesse.
- Valore intrinseco: stabilire il valore intrinseco di una cripto o di una società può essere molto difficile, e la capitalizzazione di mercato di una società non tiene sempre conto di quello che potrebbe essere il suo valore intrinseco, ovvero del valore delle attività della società, della qualità della gestione e delle prospettive future della società. Ciò significa che la capitalizzazione di mercato potrebbe non essere una misura accurata del valore.
- Comparazioni: la capitalizzazione di mercato può essere utilizzata per confrontare crypto e le società di diversi settori, ma questo confronto potrebbe essere fuorviante a causa delle differenze nei modelli di business, nei flussi di cassa e in altri fattori.
- Mancanza di regolamentazione: una delle critiche mosse da alcuni analisti riguarda il fatto che le criptovalute sono spesso meno regolamentate rispetto alle società quotate in borsa, il che significa che ci sono meno requisiti di trasparenza e reporting. Ciò può rendere difficile per gli investitori valutare il vero valore di una criptovaluta.

In sintesi, la capitalizzazione di mercato può essere utilizzata come indicatore delle dimensioni di una criptovaluta rispetto ad altre criptovalute o per valutare le dimensioni di una società rispetto ad altre società, ma non dovrebbe essere utilizzata come unica misura del valore di una criptovaluta. È importante considerare anche altri fattori, come la volatilità, le differenze di prezzo sui diversi Exchange e la mancanza di rfondamenta solide nella valutazione di alcune

criptovalute.

Market Correction

Correzione

Livello: intermedio

Argomento: finanza

Normalmente per correzione si intende il movimento al ribasso del corso di un titolo che si verifica all'interno di un movimento rialzista del mercato, mentre la correzione al rialzo che si verifica nel corso di un movimento al ribasso è denominata rimbalzo. Si ha correzione quando il movimento non è tale da far invertire il trend dominante.

Market liquidity

Liquidità di mercato

Livello: intermedio

Argomento: finanza

È la capacità di vendere o acquistare un bene senza causare grandi impatti sul prezzo di mercato. È anche legato all'idea di quanto sia facile convertire un asset in valuta fiat. Gli immobili o i beni difficilmente convertibili in denaro non sono liquidi, mentre quelli che possono essere scambiati subito sono considerati attività liquida. I mercati sono considerati liquidi quando un trader o un investitore può vendere o acquistare prontamente un determinato asset, il che significa che c'è sempre una controparte disposta a negoziare. Al contrario, un mercato che non è considerato liquido richiederebbe al trader di aspettare molto più a lungo prima che il suo ordine venga finalmente eseguito

Market maker

Livello: avanzato

Argomento: finanza

Un market maker è un trader di una borsa o exchange che scambia regolarmente grandi quantità di asset. Questo attore è di solito una grande istituzione finanziaria. Il market maker mantiene gli ordini aperti sia per comprare che per vendere un'attività all'interno di un particolare mercato. La differenza tra i prezzi di acquisto o di vendita sarà uguale allo spread bid-ask dell'asset.

Il market maker guadagna vendendo l'asset a un prezzo inferiore a quello a cui lo compra. Questa strategia di solito non considera se ci si aspetta che l'asset salga o scenda di valore a lungo termine. I market maker aiutano i

mercati aggiungendo liquidità e restringendo lo spread bid-ask (denaro-lettera). Entrambi questi fattori significano meno slippage per gli altri trader del mercato.

Gli exchange daranno spesso ai market maker una struttura di commissioni unica per incentivare l'attività di trading che rende il loro mercato più efficiente. Ai market maker può essere richiesto di soddisfare determinati criteri di trading per essere riconosciuti come market maker.

Mentre i singoli investitori comprano e vendono i loro asset preferiti nelle borse valori e nelle criptovalute, i market maker lavorano dietro le quinte per garantire che il processo vada liscio. I market maker sono responsabili dell'iniezione di liquidità in un mercato e del suo mantenimento per tutta la giornata di trading, oltre a contribuire a mantenere il mercato equo e ordinato secondo la SEC (Securities and Exchange Commission).

MASF

Acronimo di: Miner-activated softfork

Softfork attivato dai miner

Livello: intermedio

Argomento: tecnologia

Quando la maggioranza dei miner si aggiorna per applicare nuove regole, si parla di un soft fork attivato dai miner, MASF o miner-activated soft fork.
Fino al BIP141 (SegWit), la maggior parte degli aggiornamenti non critici alle regole di consenso di Bitcoin sono stati effettuati tramite soft fork attivati dai miner.
I miner si sono sempre preoccupati di essere ben coordinati tra loro in modo da non minare blocchi non validi, ma ciò ha anche permesso loro di determinare quali regole di consenso implementare. Dal punto di vista della governance, ciò significava che i grandi miner potevano porre il veto a certi aggiornamenti nonostante tali aggiornamenti avessero un ampio supporto della comunità. Per attivare SegWit, gli utenti hanno iniziato a cercare modi alternativi per bilanciare il peso della gestione del consenso da parte dei miner, e a quel punto è nata l'esigenza di distinguere i fork attivati dagli utenti, UASF, da quelli attivati dai miner o MASF.

MAST

Acronimo di: Merklized Abstract Syntax Tree

Livello: avanzato

Argomento: tecnologia

È un aggiornamento a Bitcoin introdotto con Taproot, che aggiunge agli script delle transazioni flessibilità, scalabilità e privacy. Viene utilizzato un Merkle

tree per codificare condizioni complesse all'interno delle transazioni, che prima non erano possibili a causa delle dimensioni dello script e del codice, migliorando la privacy perché possono essere introdotti nella struttura del merkle tree dei rami che rimangono nascosti.

Master fingerprint

Livello: avanzato

Argomento: tecnologia

Il Master fingerprint, che viene usato quando si crea un wallet e del quale è opportuno tenerne traccia quando si fa un backup, è un codice utile per verificare che si è ripristinato il wallet corretto.

È l'impronta della Master Key, identifica la chiave privata master del keystore ed è la stessa indipendentemente dal derivation path.

Al termine dell'importazione, è buona norma prendere nota del Master fingerprint.

La fingerprint è unica per il portafoglio a cui si accede tramite le 24 parole e la passphrase.

Master key

Livello: avanzato

Argomento: tecnologia

La Master Key, o chiave master, in un wallet HD, gerarchico-deterministico, è la chiave principale dalla quale vengono generate, o derivate, un alberto di chiavi.

La sua struttura gerarchica assomiglia a quella di un albero, con la Master Key che "determina" le coppie di chiavi che la seguono nella gerarchia.

Le prime Master Key vengono create inserendo un seed nella funzione di hash HMAC-SHA512.

La funzione HMAC restituisce 64 byte di dati (totalmente imprevedibili). Li dividiamo in due metà per creare la nostra chiave privata estesa master:

- La metà sinistra sarà la chiave privata, che è come qualsiasi altra chiave privata.
- La metà destra sarà il chain code, che sono semplicemente 32 byte extra di dati casuali.

Il chain code è necessario per la generazione di chiavi figlie. Se si entra in possesso della chiave privata ma non del chain code, non si è in grado di ricavare le chiavi discendenti, che sono quindi così protette.

Masternodes

Livello: intermedio

Argomento: tecnologia

Nodi su una rete che spesso richiedono un importo minimo di una determinata moneta in stake per accedere ai relativi premi. Possono partecipare alla governance e al voto. Questa tecnica è stata resa popolare inizialmente dalla criptovaluta Dash.

Max supply

Livello: intermedio

Argomento: politica

Il Max Supply, o offerta massima, di una criptovaluta rappresenta la quantità massima di monete o token che verranno mai create per quella specifica criptovaluta. Questo valore è solitamente predefinito nel protocollo sottostante della criptovaluta e può variare da un progetto all'altro.

Per quanto riguarda Bitcoin, l'offerta massima è stata fissata a circa 21 milioni di BTC. Questo significa che una volta che saranno stati estratti o minati tutti i 21 milioni di Bitcoin, non ne verranno mai creati altri.
Attualmente, la quantità di Bitcoin in circolazione aumenta gradualmente attraverso il processo di estrazione, ma ci sarà un momento, ipotizzato circa nell'anno 2140, in cui si raggiungerà il limite massimo di 21 milioni e non ci saranno ulteriori nuove creazioni.

La scelta di impostare un'offerta massima fissa come quella di Bitcoin è stata fatta per garantire la scarsità dell'asset e per limitare l'inflazione nel lungo termine. Questa limitazione della fornitura può avere un impatto sul valore di Bitcoin, poiché l'aumento della domanda e l'offerta limitata possono potenzialmente portare a un apprezzamento del prezzo nel tempo.

Stabilire un tasso di emissione costante insieme a un'offerta massima predefinita può essere utile per controllare il tasso di inflazione di una criptovaluta, che potenzialmente può portare a un apprezzamento a lungo termine dell'asset.

In generale, quando si raggiunge l'offerta massima, ci saranno meno monete disponibili sul mercato.

Ci si aspetta che ciò crei una condizione di scarsità di mercato, che potrebbe alla fine portare a una deflazione (o a un tasso di inflazione dello 0%).

Tuttavia, alcune criptovalute non hanno un'offerta massima predefinita, il che significa che possono essere continuamente estratte o coniate.
Un esempio di criptovaluta senza un'offerta massima predeterminata è Ethereum. L'offerta di Ether aumenta costantemente con la generazione di nuovi blocchi.

I 21 Milioni di Bitcoin Ci sono diverse ipotesi sulla scelta di 21 milioni di bitcoin come max supply.
Tra queste, c'è la testimonianza di Ray Dillinger, sencondo il quale con Satoshi Nakamoto e Hal Finney discutevano sul total supply.
Allora, nel 2008, il valore globale della massa monetaria M1 o liquidità primaria (banconote e monete di tutte le valute fisiche in circolazione, depositi bancari e altre forme di denaro altamente liquide) secondo il report della CIA era circa 21 mila miliardi di dollari, ovvero 21 con 12 zeri.
Finney osservò allora che la divisione più piccola del dollaro era il centesimo, e quindi l'M1 mondiale in centesimi di dollaro era 21 con 14 zeri dopo, che corrisponde ai 21 000 000 000 000 00 di unità più piccole di bitcoin (ovvero satoshi che però allora non si chiamavano ancora così)

Maximalist

Massimalista

Livello: base

Argomento: politica

Il termine massimalista si applica di solito ai bitcoin: i massimalisti Bitcoin, a volte abbreviati in bitcoin maxi, credono che esso sia l'unica criptovaluta che sarà necessaria nel futuro e che tutte le altre criptovalute siano inferiori, inutili o addirittura dannose, definendo spesso tutte le altcoin come shitcoin.
Il termine massimalista viene utilizzato con meno frequenza anche per altre critpo, ad esempio ci sono i massimalisti ethereum.

Il termine massimalista, maximalist in inglese, si riferisce a una persona che crede in obiettivi o ideali estremi o radicali. I massimalisti spesso si rifiutano di accettare compromessi e sono disposti a lottare per i loro obiettivi.
In politica, i massimalisti sono spesso associati a movimenti rivoluzionari o radicali.

Nonostante il termine possa avere connotazioni negative, alcuni sostenitori di Bitcoin si definiscono massimalisti quasi con orgoglio.

Massimalista tossico L'aggettivo "tossico" è spesso aggiunto per indicare che questa posizione estremista può sfociare in un comportamento negativo, aggressivo e ostruzionistico.
Un massimalista tossico Bitcoin può essere una persona che respinge qualsiasi discussione o critica nei confronti di Bitcoin, e considera che anche solo parlare di ogni qualunque altra criptovaluta o progetto possa essere dannoso.
Possono essere inclini a attaccare verbalmente coloro che dissentono dalle loro opinioni e possono contribuire a un clima di divisione e conflitto all'interno della comunità e isolamento della comunità nei confronti di chi non ne fa parte.

Ecco alcuni consigli per evitare di diventare un massimalista tossico Bitcoin:

- Sii aperto al dialogo e alle critiche
- Evita di fare affermazioni esagerate
- Sii rispettoso delle persone che non sono d'accordo con te
- Concentrati sui fatti e sui dati, non sulle emozioni

Medium of Exchange

Mezzo di scambio

Livello: base

Argomento: economia

In economia il termine "medium of exchange", traducibile come "mezzo di scambio" ma anche "moneta merce" anche se questa è meglio tradotta in inglese come "commodity money", si riferisce a un bene o strumento che viene utilizzato per facilitare la compravendita di beni e servizi in un'economia.
In altre parole, è un mezzo attraverso il quale le persone possono scambiare valore tra loro.

Il denaro ha come funzione primaria e in effetti unica essenziale quella di mezzo di scambio. Tradizionalmente, le valute fiat, come il dollaro americano, l'euro o lo yen, sono esempi di mezzi di scambio comunemente accettati nelle transazioni quotidiane. Le persone accettano queste valute in quanto hanno fiducia nella loro stabilità e nella loro capacità di conservare il valore nel tempo.

Inizialmente, Bitcoin è stato concepito come un mezzo di scambio digitale peer-to-peer, consentendo alle persone di inviare e ricevere pagamenti in modo rapido ed economico senza intermediari.
I bitcoin sono un mezzo di scambio in quanto possono essere utilizzati per acquistare beni e servizi da un numero crescente di commercianti. Ad esempio, è possibile acquistare beni e servizi online con bitcoin, oppure è possibile utilizzarli per pagare per beni e servizi in negozi fisici che li accettano presenti praticamente in ogni parte del mondo, anche se sono una piccola minoranza.

Tuttavia, la capacità dei bitcoin di essere utilizzati come mezzo di scambio è ancora limitata e la definizione applicata a Bitcoin nel corso del tempo ha sollevato discussioni e diatribe, anche in funzione del ruolo che dovrebbero svolgere nell'economia.
Ci sono alcune sfide da considerare quando si tratta di considerare Bitcoin come medium of exchange:

- **Volatilità**: Una delle principali sfide di Bitcoin come medium of exchange è la sua notevole volatilità. Il valore di Bitcoin può oscillare drasticamente in breve tempo. Questa volatilità rende difficile stabilire prezzi e fare acquisti quotidiani in Bitcoin, poiché il suo valore può variare notevolmente prima che la transazione sia completata.
- **Adozione limitata**: Nonostante il crescente interesse e l'adozione di Bitcoin, non è ancora ampiamente accettato come metodo di pagamento in

molte parti del mondo. La mancanza di accettazione generalizzata limita la sua utilità come medium of exchange.
- **Scalabilità e costi delle transazioni**: A causa della congestione della rete e dei costi delle transazioni variabili, Bitcoin potrebbe non essere sempre la scelta più conveniente per le transazioni di piccolo valore; esistono comunque delle soluzioni quali Lightning Network che possono in determinati casi risolvere tali problemi.

I sostenitori dei bitcoin come mezzo di scambio sottolineano che i bitcoin hanno il potenziale per essere un mezzo di scambio più efficiente ed economico delle valute fiat.
I bitcoin sono disponibili 24 ore su 24, 7 giorni su 7, e le transazioni in bitcoin sono generalmente più economiche delle transazioni digitali con valute fiat, i bitcoin possono essere utilizzati in qualunque parte del mondo e non sono censurabili.

Bitcoin come Medium of Exchange vs. Store of Value La diatriba riguardo a considerare Bitcoin come medium of exchange contro store of value si basa sulla sua natura unica. Alcuni ritengono che Bitcoin sia più adatto a essere un "store of value" (deposito di valore), simile all'oro, poiché molti investitori lo trattano come un'alternativa digitale all'oro come un modo per conservare il proprio patrimonio e proteggerlo dall'inflazione. Altri sostengono che Bitcoin possa ancora evolvere per diventare un medium of exchange più efficace, ma che attualmente presenta delle limitazioni.

In ultima analisi, la posizione di Bitcoin come medium of exchange o store of value dipenderà in gran parte da come evolverà nel tempo e dalla sua accettazione nell'economia globale. Alcune persone possono utilizzarlo come un mezzo di scambio, mentre altre lo terranno come una forma di investimento. La discussione continua a evolversi a misura che Bitcoin e altre criptovalute guadagnano ulteriore adozione e maturità.

Meme coin

Livello: intermedio

Argomento: finanza

Le "meme coin" sono criptovalute che nascono con la strategia di marketing di capitalizzare il successo di meme diventati virali sul web, legati a fenomeni sociali, scherzi o contenuti popolari online. Il contenuto virale stesso diventa il volto, e spesso il logo, identificativo della moneta.

Il caso più noto è il Dogecoin, creato nel 2013 come scherzo e ispirato al famoso cane Shiba Inu, una razza giapponese a pelo folto e di colore ocra. Il Dogecoin ha registrato notevoli rialzi, principalmente attribuiti ai tweet di Elon Musk. A seguito di questo successo, sono emerse altre "meme coin" come Shiba Inu, raffigurante la stessa razza di cane nel logo di Dogecoin, e Floki Inu, che prende

il nome dal personaggio della serie televisiva Vikings, oltre a essere il nome del cane di Elon Musk. Le "meme coin" sono generalmente criptovalute che non dispongono di una propria blockchain e si appoggiano spesso alla rete Ethereum o Binance Smart Chain.
Con l'introduzione degli Ordinal su Bitcoin, si è visto crescere questo fenomeno anche sulla block chain bitcoin.

In primo luogo, l'utilizzo di meme e altri contenuti virali le rende attraenti per un pubblico più vasto, anche per coloro che non sono esperti di criptovalute. In secondo luogo, la loro volatilità offre la possibilità di guadagni rapidi, il che può essere allettante per gli investitori. Tuttavia, è importante sottolineare che i rischi legati alla volatilità sono elevati, poiché i prezzi possono essere imprevedibili, portando gli investitori a perdere ingenti somme di denaro in breve tempo. Inoltre, molte "meme coin" spesso mancano di un team di sviluppo solido e di una base di utenti stabile, aumentando la probabilità di fallimento. Infine, sono frequentemente bersaglio di truffe e manipolazioni, richiedendo agli investitori di prestare molta attenzione per evitare frodi.

L'ascesa dei social media e delle comunicazioni online ha facilitato la rapida diffusione delle "meme coin".

Mempool

Livello: intermedio

Argomento: tecnologia

Il termine mempool è la contrazione di memory pool.

È quella zona di memoria, una specie di area di attesa, dove i nodi tengono le transazioni che non sono ancora confermate (pending), ovvero che non sono state ancora inserite in un blocco della blockchain, in attesa di essere prelevate da un miner che le inserisca in un blocco e aggiunga questo blocco alla blockchain.

Non esiste una mempool condivisa tra i nodi, anche se le mempool dei vari nodi tendono a convergere come contenuto: le transazioni Bitcoin vengono trasmesse attraverso un sistema distribuito asincrono tra i vari nodi che gestiscono la propria mempool e ci memorizzano le transazioni da confermare ricevute dagli altri nodi, e le mantengono in base a regole e parametri impostati nel proprio software.

I nodi devono verificare che le transazioni all'interno del mempool siano valide verificando schemi di firma corretti, che gli output non superino gli input e che i fondi non siano stati spesi due volte.

Le transazioni che si trovano nella mempool vengono anche chiamate 0-conf, perché non hanno ancora ricevuto una conferma.

Le transazioni nella mempool possono essere sostituite, un processo che viene chiamato unconfirmed transaction replacement, ad esempio modificate tramite

il meccanismo RBF Replace by Fee, che consente a chi ha creato la transazione di incentivare i miner ad inserire prima la transazione in blockchain aumentando le fee.

Anche il destinatario della transazione può incentivare i miner a confermare la transazione attraverso CPFP Child pays for parent.

L'idea che una transazione che rimane troppo tempo nella mempool senza essere confermata scada, è sbagliata.

Il protocollo bitcoin non ha una regola per far scadere le transazioni che sono nella mempool e che non sono state confermate, in pratica non esiste un campo time che possa essere usato per fare in modo che si possa far scadere dopo un certo periodo di tempo una transazione in attesa di essere confermata. Una volta creata una transazione Bitcoin, non scade mai automaticamente. In teoria si potrebbe creare una transazione che rimane bloccata a 0 conferme per alcuni anni, e poi all'improvviso essere inserita in un blocco e quindi confermata.

Ogni full node bitcoin ha una sua mempool, che di default non supera i 300 Mbyte ma tale dimensione può essere impostata per ogni nodo. Si può vedere usando il comando:

```
bitcoin-cli getmempoolinfo
```

che visualizza nel campo maxmempool il valore impostato come dimensione della mempool.

Questo spazio non misura quanto occuperanno effettivamente le transazioni nel blocco, ma la memoria necessaria dal software per gestire questi dati, e dipende anche dalla piattaforma utilizzata per far girare il software del nodo.

Teniamo conto che ogni nodo si collega a diversi nodi peer e a questi farà il relay delle nuove transazioni che riceve. Quando la coda di transazioni (backlog) del nodo arriva a raggiungere l'occupazione di memoria del valore di maxmempool, elimina le transazioni con le feerate più basse e aumenta il suo minMempoolFeeRate. Comunica il nuovo minMempoolFeeRate ai suoi peer, dicendo loro essenzialmente di non inoltrare transazioni con una feerate inferiore per il momento.

Ogni nodo agisce individualmente, quindi un nodo con un mempool più grande o un'architettura diversa potrebbe eliminare le transazioni prima o dopo. Inoltre, i nodi mantengono una copia delle transazioni rilevanti per il proprio wallet. Anche se tutti gli altri nodi hanno eliminato una transazione, il mittente e i destinatari della transazione ne conservano una copia. Quindi, se la transazione è tua o sei il destinatario, continuerai a vederla come pending o on-chain quando confermata.

Dopo che il backlog diminuisce al punto che la memoria necessaria è inferiore alla maxmempool impostata e con un certo ritardo aggiunto, un nodo diminuirà il proprio minMempoolFeeRate e ricomincerà ad accettare le transazioni che in precedenza aveva espulso.

Il nodo di Bitcoin Core ha il parametro `mempoolexpiry` che indica il numero di ore dopo le quali le transazioni vengono rimosse dalla mempool, ed è impostato di default a 336 ore ovvero 2 settimane (precedendemente era 72 ore); ogni nodo può impostare liberamente questo parametro.

Bisogna quindi considerare che anche se la maggior parte dei nodi dovesse dimenticare una transazione, ovvero cancellarla dalla mempool, non significa che tutti debbano farlo o lo faranno.

La possibilità che una transazione possa, in un certo modo, scadere comunque esiste: quando si trasmette una transazione, si invia un frame tx a tutti i peer connessi. Questi peer memorizzano la transazione nella loro mempool e dicono a tutte le loro connessioni che hanno una nuova transazione. Quando quelle connessioni non ce l'hanno ancora, la chiedono, ed è così che una transazione si diffonde nella rete dei nodi bitcoin. Ad un certo punto ogni nodo della rete avrà la transazione nella sua mempool, e a quel punto non sarà più inviata sulla rete.

Da Bitcoin Core 0.14.0, la mempool è salvata su disco, quindi persiste anche dopo il riavvio. Nelle versioni precedenti, un riavvio comportava anche la cancellazione del mempool.

Se la mempool viene cancellata, ne viene forzata la cancellazione, o viene cancellata per superamento della memoria o per altri motivi, e la transazione viene eliminata dai vari nodi, queste condizioni rendono molto improbabile che la transazione sparisca dall'intera rete, ma non impossibile.

A partire da Bitcoin Core 0.14.0, questi sono i modi per cui una transazione può lasciare la mempool:

- La transazione è stata inclusa in un blocco.
- La transazione o uno dei suoi antenati non confermati è in conflitto con una transazione inclusa in un blocco.
- La transazione è stata sostituita da una versione più recente, ad esempio tramite RBF
- La transazione si trovava in fondo alla mempool (se ordinata per feerate ovvero in base alle fee per dimensione), il mempool ha raggiunto il suo limite di dimensione (vedere l'opzione -maxmempool) e una nuova transazione a tariffa più alta è stata accettata, sfrattando quella in fondo.
- La transazione è scaduta per timeout (per impostazione predefinita, 14 giorni dopo l'inserimento).
- Inoltre, le transazioni che hanno lasciato la mempool possono sempre rientrarvi. Ad esempio, quando fanno parte del portafoglio locale e vengono ritrasmesse, o quando vengono ricevute di nuovo attraverso la rete. Lo sfratto non implica l'annullamento di una transazione.

mempool sniping

Livello: avanzato

Argomento: tecnologia

mempool sniping è una forma di attacco che sfrutta la mempool Bitcoin, l'area di attesa per le transazioni Bitcoin non confermate.
In questa forma di attacco, l'attaccante viene chiamato sniper.

In particolare, si tratta di monitorare il mempool per le transazioni Ordinal di valore, come la creazione o lo scambio di NFT o token basati su Ordinals, e sostituire se stessi come pagatori di tali transazioni, modificando l'indirizzo del destinatario e aumentando leggermente la commissione.

Il mempool sniping sfrutta le transazioni PSBT, o parzialmente firmate, comunemente utilizzate dalla maggior parte dei mercati Ordinals.
La vulnerabilità sorge quando la transazione parzialmente firmata di un venditore può essere intercettata da qualsiasi acquirente, consentendogli di sostituire i dettagli dell'acquirente con i propri.
Impiegando una commissione più elevata, la transazione del nuovo acquirente ottiene la priorità, con conseguente sniping di successo.

In questo modo, si aumenta la probabilità che il miner scelga la transazione dello sniper per l'inclusione nel prossimo blocco, lasciando la transazione originale non confermata e lo sniper con il nuovo asset Ordinal.

mempoolminfee

Livello: avanzato

Argomento: tecnologia

Il **mempoolminfee** è un parametro che può essere impostato in un nodo Bitcoin per determinare la fee minima che una transazione deve pagare per essere accettata nella mempool del nodo.
La mempool è l'elenco delle transazioni che sono in attesa di essere confermate e aggiunte dai miner alla blockchain.

In pratica, il mempoolminfee è la fee minima che gli utenti dovrebbero pagare per garantire che la loro transazione venga presa in considerazione per essere elaborata e aggiunta alla blockchain. Se la fee della transazione è inferiore al valore impostato nel mempoolminfee del nodo, la transazione potrebbe essere ignorata e non trasmessa alla rete bitcoin e quindi arrivare al miner.

È un limite inferiore indipendente per l'accettazione della mempool di un nodo che aumenta dinamicamente quando il limite della memoria della mempool (maxmempool) viene superato.

Il valore del mempoolminfee può variare a seconda del nodo e delle condizioni di mercato, come la domanda di transazioni e la capacità della rete. In genere, durante i periodi di congestione della rete, il mempoolminfee potrebbe essere aumentato per pulire (purge) la mempool dalle transazioni che hanno delle fee

più basse, mentre durante i periodi di bassa domanda potrebbe essere ridotto per mantenere le tariffe competitive e attrarre gli utenti.

merged mining

Livello: avanzato

Il merged mining è una tecnica che consente ai miner di Bitcoin di minare Bitcoin e un'altra blockchain simultaneamente utilizzando la stessa funzione di hashing.
Questo metodo consente ai miner di utilizzare l'hardware e le risorse esistenti per validare sia i blocchi Bitcoin che quelli di un'altra rete contemporaneamente. Il merged mining può migliorare la sicurezza di una catena più piccola sfruttando la potenza di elaborazione di una catena più grande come Bitcoin, riducendo il rischio di attacchi del 51% man mano che più miner lo adottano.

Quando un miner trova un blocco per Bitcoin, la stessa proof-of-work può essere inviata a un'altra blockchain. Se la soluzione è valida per entrambe, il miner guadagna ricompense da entrambe le blockchain.

Il merged mining comporta l'estrazione di due o più criptovalute simultaneamente senza sacrificare le prestazioni di mining. Tramite Auxiliary Proof of Work (AuxPoW), un miner può utilizzare la potenza di calcolo per minare blocchi su più catene. La blockchain madre fornisce la proof-of-work e la blockchain ausiliaria la accetta come valida.

Per eseguire il merged mining, le criptovalute coinvolte devono utilizzare lo stesso algoritmo. Ad esempio, Bitcoin utilizza SHA-256, quindi qualsiasi altra moneta che utilizza SHA-256 può essere estratta insieme a Bitcoin, a condizione che l'implementazione tecnica sia corretta. Mentre la blockchain madre non è interessata, la blockchain ausiliaria deve essere programmata per accettare il lavoro della catena madre. Aggiungere o rimuovere il supporto al merged mining in genere richiede un hard fork.

In teoria, il merged mining può essere vantaggioso per le blockchain più piccole, migliorandone la sicurezza sfruttando la potenza di hashing di Bitcoin e riducendo la probabilità di attacchi del 51% se un numero sufficiente di miner adotta questa pratica. Tuttavia, i critici sostengono che può fornire un falso senso di sicurezza. Un grande pool di mining, sebbene non dominante su Bitcoin, potrebbe facilmente controllare il 51% della potenza di hashing sulla catena più piccola. Inoltre, poiché i guadagni principali dei miner provengono da Bitcoin, potrebbero avere meno incentivi ad agire onestamente sulla catena più piccola, trascurandone potenzialmente la sicurezza.

I sostenitori ribattono che se le ricompense per il mining della catena ausiliaria sono abbastanza allettanti, attireranno più minatori, riducendo la centralizzazione e aumentando la sicurezza.

Merkle tree

Livello: avanzato

Argomento: tecnologia

Un Merkle Tree è una struttura dati che consente di avere un unico hash, chiamato root, che rappresenta una quantità anche grande di valori, e garantire tramite questo unico hash che tutti i dati non siano alterabili.

Ha una struttura ad albero, nel quale i vari rami sono a loro volta degli hash.

In un Merkle Tree ogni nodo foglia è etichettato con l'hash di un blocco di dati e ogni nodo non foglia è etichettato con l'hash crittografico delle etichette dei suoi nodi figli. Gli alberi di hash permettono una verifica efficiente e sicura del contenuto delle blockchain, poiché ogni cambiamento si propaga verso l'alto e la verifica può essere fatta semplicemente guardando l'hash superiore.

Uso di Merkle Tree in Bitcoin È una componente fondamentale della blockchain bitcoin, in quanto consente delle verifiche molto rapide, ed è usata anche su altre cripto.

Un Merkle Tree riassume tutte le transazioni in un blocco producendo un'impronta digitale (cioè un singolo hash) dell'intero insieme di transazioni.

I Merkle Tree sono utilizzati per memorizzare tutte le transazioni in un dato blocco. Il vantaggio di questo sistema è che un nodo può facilmente dimostrare ad un altro che una data transazione era contenuta in un blocco specifico. Questo è utile per i nodi SPV e i light client, che non memorizzano l'intera blockchain e sono interessati solo a certe transazioni o blocchi.

Per esempio, se un utente ha un wallet e sta aspettando la conferma della sua transazione, ma non ha un full node, può richiedere una prova Merkle ad un altro utente che gestisce un full node. Questa prova viene considerata sufficiente per stabilire che la transazione a cui è interessato l'utente sia inclusa in un blocco valido, senza che l'utente che gestisce il full node debba condividere tutte le transazioni o l'intero blocco con il richiedente.

Da un punto di vista tecnico, un Merkle Tree ha degli strati. Il primo strato è la lista di tutti i txid, gli ID delle transazioni, in un blocco. Per produrre il secondo strato, questi txid sono concatenati e sottoposti a hash a coppie usando SHA-256. Così, il secondo strato sarà lungo la metà del primo strato. Questo processo continua fino a quando l'ultimo strato contiene esattamente un hash. Questo è chiamato Merkle root. Date le proprietà di un hash, se un singolo id di transazione viene cambiato, questo cambiamento risalirà l'albero e cambierà interamente l'hash della root.

Il vantaggio di un Merkle Tree è che la presenza di qualsiasi dato id di transazione in un Merkle Tree può essere dimostrato senza rivelare l'intero Merkle Tree. Per esempio, in un Merkle Tree con otto transazioni, devono

essere forniti solo tre hash per provare che uno dei txid è stato incluso in quel Merkle Tree. Questo fornisce una grande efficienza per i Light Client, che non memorizzano l'intera blockchain, e quindi devono interrogare altri nodi per la prova che certe transazioni sono confermate.

Merkle-Sum Tree

Livello: avanzato

Argomento: tecnologia

Un Merkle Sum Tree è un tipo di Merkle tree che rende efficiente la verifica dell'assenza di cambiamenti nel valore cumulativo o nella distribuzione delle foglie di un Merkle tree.

Questa proprietà si ottiene inserendo valori numerici in ogni foglia dell'albero e sommando poi tali valori nel ramo sovrastante. Alla fine, la root dell'albero Merkle-Sum contiene la somma dei valori totali dell'albero.

Ogni livello del Merkle tree contiene anche l'hash dei due rami sottostanti, come in un normale Merkle tree. Pertanto, la root del Merkle tree contiene un singolo hash e un valore numerico. Finché l'hash non cambia, nessun dato dell'albero è cambiato, e finché il valore numerico non cambia, la somma di tutte le foglie dell'albero non è cambiata. Questi due dati consentono agli osservatori di verificare in modo efficiente la composizione totale e le riallocazioni di un asset senza dover verificare la posizione di ogni unità dell'asset.

Merkle sum tree sono un tipo di merkle tree che contiene valori numerici a ogni foglia e ogni nodo contiene anche la somma dei valori sottostanti. Alla root del Merkle sum tree si trova la somma dei valori totali dell'albero.

I Merkle sum tree consentono di verificare in modo efficiente la conservazione (non inflazione) effettuando il commit sulle quantità associate alle foglie.

Metaverse

metaverso

Livello: base

Argomento: tecnologia

Il termine metaverso è composto dal prefisso "meta" (che significa oltre) e dalla radice "verso" (una formazione posteriore da "universo"); il termine è tipicamente usato per descrivere il concetto di una futura iterazione di Internet, composta da spazi virtuali 3D persistenti, condivisi, collegati in un universo virtuale percepito, nel caso dei metaverse basati su blockchain possono consentire di esporre, promuovere, valorizzare e costruire parti del metaverso. All'interno dei metaversi, ogni utente ha il proprio avatar personalizzabile, sceglie le caratteristiche tra quelle offerte dalla piattaforma, con la possibilità di muoversi nel

mondo virtuale in costruzione o di essere parte attiva del suo sviluppo, attraverso l'acquisizione di spazio e asset virtuali con l'obiettivo di costruire un personale "ambiente virtuale ideale".

MEV

Acronimo di: Miner extractable value

Livello: avanzato

Argomento: tecnologia

Il MEV, Miner extractable value o valore estraibile dal miner, misura i ricavi che si possono ottenere dalle attività di produzione dei blocchi della blockchain da parte dei miner che va oltre il tipico reddito delle fee o commissioni controllando quali transazioni includere, escludere e l'ordinamento delle transazioni all'interno di un determinato blocco.

I miner controllano tutte queste cose - inclusione, esclusione e ordine delle transazioni - ma non sono gli unici a guadagnare MEV.

I **Searcher** sono partecipanti alla rete che monitorano l'attività delle transazioni on-chain per opportunità di MEV. Queste opportunità vengono in genere inviate automaticamente ai miner dai bot di un Searcher con fee più elevate del normale associate alle transazioni MEV per garantire che vengano inserite in un nuovo blocco incentivando finanziariamente i miner a farlo, il che consente di estrarre con successo il valore. Pertanto, i miner e i Searcher generalmente condividono le entrate derivanti da una determinata opportunità MEV.

Va detto che c'è qualche disaccordo su cosa significhi MEV. Tradizionalmente, il termine rappresenta il valore estraibile del miner, ma alcuni sviluppatori hanno recentemente iniziato a riferirsi a MEV come *Maximal Extractable Value*, valore estraibile massimo per includere forme di estrazione del valore on-chain non specifiche per il mining.

Nei sistemi basati sulla Proof of work, *Miner Extractable Value* è un termine che descrive i profitti che i miner possono guadagnare manipolando il modo in cui le transazioni vengono priorizzate, escluse, riorganizzate o alterate nei blocchi che estraggono.
Tuttavia, dall'aggiornamento di Ethereum a Ethereum 2.0, che ha spostato la rete alla proof-of-stake, il concetto di MEV ha assunto un nuovo nome e viene ora indicato come *Maximal Extractable Value* nei sistemi proof-of-stake. In questo contesto, sono i proponenti dei blocchi anziché i miner, che sono i validatori, ad avere l'opportunità di estrarre questo valore.

I miner (o validatori in Ethereum) hanno il ruolo di confermare le transazioni inserendole nei blocchi. La loro posizione li pone in una posizione privilegiata rispetto agli altri utenti e consente loro di determinare l'ordine finale delle transazioni nella blockchain.
All'interno di un blocco, le transazioni sono generalmente ordinate con le fee più

alte in alto, ma di tanto in tanto si aprono opportunità che consentirebbero ai miner di ottenere un profitto aggiuntivo modificando strategicamente l'ordine delle transazioni a proprio vantaggio.

Qual è il problema nel lasciare che i miner traggano in questo modo un po' di profitto extra?
Le preoccupazioni iniziano a emergere solo quando alcuni di questi miner, quelli dotati di capacità analitiche più avanzate e di computer più potenti, riescono a identificare e sfruttare le opportunità di profitto MEV in modo più efficace di altri.

Queste opportunità potrebbero non essere sempre facili da individuare, ma maggiore è il valore che può essere estratto attraverso l'analisi della chain, più forte diventa l'incentivo per i team di ricerca dotati di bot a svolgere questo lavoro. Nel corso del tempo, questa disparità nella capacità di realizzare profitti dei miner crea una tendenza verso la centralizzazione all'interno della rete. In definitiva, minando il principio fondamentale della blockchain: la decentralizzazione.

Questo è esattamente lo scenario che la comunità degli sviluppatori Bitcoin mira a prevenire quando considera il modo migliore per gestire una maggiore espressività degli smart contract Bitcoin.

Un punto chiave della attuale differenza tra Bitcoin ed Ethereum è la visibilità delle transazioni. A differenza di Ethereum, non tutti gli aspetti del contratto sono necessariamente trasparenti, il che significa che i miner Bitcoin non hanno la stessa capacità di vedere lo stato interno del contratto e di gestirlo in anticipo.

Molti utenti temono che se rendiamo tecnicamente possibili i contratti di livello 2, il MEV diventerà inevitabile.

Esistono diversi fattori che contribuiscono al MEV:

- trasparenza della mempool
- trasparenza dello smart contract
- espressività dello smart contract

MiCA

Acronimo di: Markets in Crypto-Asset Regulation

Livello: avanzato

Argomento: politica

Il Regulation on Markets in Crypto-assets, è il regolamento Europeo sui mercati nelle criptovalute, abbreviato come MiCA o **MiCAR**, dovrebbe portare all'adozione nell'Unione europea di una cornice normativa armonizzata per i mercati delle cripto-attività e introdurre nuovi requisiti di licenza.

Approvato con la votazione finale dal parlamento Europeo il 20 aprile 2023, e adottato dal Consiglio dell'UE a maggio 2023, si dovrà poi attendere altri 12

mesi (per le stablecoin) e 18 mesi (per tutto il resto del regolamento) perché MiCAR si applichi effettivamente.
L'ESMA, l'autorità di regolamentazione delle security dell'UE, produrrà poi una guida sui dettagli dell'applicazione del regolamento.
Per vedere MiCAR applicato nella sua interezza occorrerà dunque aspettare il secondo semestre del 2024. Il MiCAR intercetterà solo in parte la dimensione "digitale" dei nuovi mercati, e non si applicherà ai provider di soluzioni tecnologiche.

Verranno introdotte regole per emittenti, offerenti e prestatori di servizi in cripto-attività, tra cui gli exchange, le piattaforme di trading e i fornitori di servizi di custodia di criptovalute.

Il MiCA introduce diverse definizioni relative ai cripto-asset, tra le quali la stessa definizione di cripto-asset:

- **Crypto-assets** sono definiti come rappresentazioni digitali di valore o diritti che possono essere trasferiti e memorizzati elettronicamente utilizzando la tecnologia distributed ledger o una tecnologia simile.

Gli asset crittografici (crypto-assets) sono definiti come asset digitali che possono dipendere dalla crittografia ed esistere su un registro distribuito. Una tassonomia di base distingue tra:

- payment token o token di pagamento (mezzi di scambio o pagamento)
- investment token o token di investimento (hanno diritti di profitto associati)
- utility token o token di utilità (consentono l'accesso a un prodotto o servizio specifico).

e più precisamente vengono definite le seguenti categorie di cripto-asset:

- **Utility Token** è definito come un tipo di cripto-asset che è destinato a fornire accesso digitale a un bene o servizio, disponibile su DLT ed è accettato solo dall'emittente di quel token.
- **ARTs Asset-referenced token** si intende un tipo di cripto-asset che mira a mantenere un valore stabile facendo riferimento al valore di diverse valute fiat che hanno corso legale, una o più materie prime, o uno o più cripto-asset, o una combinazione di tali asset.
- **EMTs e-money tokens** è definito come un tipo di cripto-asset il cui scopo principale è quello di essere utilizzato come mezzo di scambio e che mira a mantenere un valore stabile facendo riferimento al valore di una valuta fiat, o official currency per usare il gergo del MiCAR.

Una disciplina di dettaglio è poi prevista per le stablecoin, distinguendo tra EMT e-money token e quelle ancorate ad altri asset, o ART asset-referenced token: si tratta di requisiti organizzativi e prudenziali, oltretutto graduati in senso più restrittivo se la stablecoin è *significativa* per dimensioni o interconnessione con il sistema finanziario.

La supervisione su ART ed EMT sarà affidata alle autorità nazionali, con il trasferimento di competenze all'EBA se la stablecoin diventa significativa.

Si definiscono, inoltre, forme di monitoraggio e restrizioni per prevenire un ampio utilizzo degli ART come mezzo di scambio; in sede di autorizzazione e di supervisione ongoing è previsto che la BCE e, se del caso, le banche centrali degli Stati membri non-euro, adottino pareri vincolanti per tutelare la sovranità monetaria, la trasmissione della politica monetaria e il regolare funzionamento del sistema dei pagamenti.

I responsabili politici dell'ECON, European Parliament Committee on Economic and Monetary Affairs o Commissione per gli affari economici e monetari del Parlamento europeo, hanno approvato ad ottobre 2022 accettato la legislazione MiCA, risultato dei negoziati a tre tra il Consiglio dell'UE, la Commissione europea e il Parlamento europeo. I membri della commissione parlamentare hanno approvato la politica quadro sulle criptovalute con un voto di 28 favorevoli e un contrario

Secondo l'accordo i CASP, fornitori di servizi di criptovalute, per operare all'interno della regione europea dovranno aderire a severi requisiti giustificando tali requisiti secondo la solita formula dell'esigenza di proteggere i consumatori, e possono anche essere ritenuti responsabili in caso di perdita di criptovalute degli investitori. I CASP più grossi che saranno monitorati dall'ESMA.

Miner

Livello: base

Argomento: tecnologia

Letteralmente minatore, termine che richiama colui che scende nelle miniere per estrarre minerali quali l'oro.

Un miner è un individuo o un'entità che partecipa al processo di estrazione dei bitcoin, utilizzando la potenza di calcolo per risolvere un particolare calcolo matematico e confermare le transazioni sulla rete bitcoin.

In cambio, i miner ricevono una ricompensa in bitcoin per ogni blocco che risolvono. Questo processo è noto come Mining e consente di generare nuove unità di bitcoin, mantenere la sicurezza della rete e confermare le transazioni.

La ricompensa del miner viene chiamata Block Reward che è composto da:

- Block Subsidy: la quantità di nuovi bitcoin coniati in ogni blocco
- Fee sulle transazioni: le commissioni che vengono pagate da chi effettua le transazioni

Il mining di Bitcoin si basa sull'algoritmo di Proof-of-Work, che comporta l'esecuzione di una grande quantità di calcoli alla ricerca di un valore particolare.

Questo problema matematico consiste nel trovare un numero, chiamato Nonce che, unito agli altri dati del blocco, generi un valore hash che soddisfi determinate condizioni, che inizi con un certo numero di zeri.

Il mining di Bitcoin implica quindi il calcolo di questi valori hash, che inizialmente poteva essere effettuato con la CPU dei computer, poi con l'aumentare della difficoltà i miner hanno utilizzato la GPU, e attualmente è necessario l'utilizzo di hardware specializzato ASIC.

L'hardware si interfaccia con un software che consente di specificare dove effettuare l'operazione di mining e con quali parametri.

La difficoltà è diventata talmente alta che i miner lavorano assieme attraverso le Mining pool.

Mining

Livello: base

Argomento: tecnologia

Il mining, il cui termine richiama l'analogia con l'estrazione dell'oro dalle miniere, è il processo attraverso il quale le transazioni delle criptovalute vengono raccolte, verificate e registrate nella blockchain.

Il lavoro svolto dai miner è essenziale per mantenere l'integrità della rete; il miner è anche responsabile dell'introduzione di nuove monete nel sistema.

Per molte criptovalute, l'emissione di nuove monete non è nelle mani di entità centralizzate: le nuove unità di criptovaluta vengono generate attraverso il processo di mining, che segue un insieme predefinito di regole stabilite dal protocollo sottostante.

Il protocollo definisce quali sono le regole primarie, i cosiddetti algoritmi di consenso delineano come queste regole verranno seguite (ad esempio, durante la convalida delle transazioni).

Su Bitcoin, che ha introdotto questo sistema, i partecipanti coinvolti nel processo di mining sono chiamati mining node (o semplicemente miner), e giocano un ruolo chiave nella sicurezza della rete blockchain.

Il compito di un miner è raccogliere le transazioni non confermate dalla mempool e organizzarle in un blocco candidato, che cercheranno di convalidare. Quando il miner crea un blocco candidato, include una transazione in cui invia a se stesso il premio del blocco. Questa transazione è nota come transazione coinbase ed è spesso la prima ad essere registrata in un blocco.

Poiché il processo di mining richiede enormi capacità di elaborazione, i miner spesso lavorano insieme coordinandosi attraverso le mining pool.

Mining pool

Livello: intermedio

Argomento: tecnologia

Una mining pool è un gruppo di miner che lavorano assieme per estrarre Bitcoin o altre criptovalute e condividono così i premi proporzionalmente all'hash rate fornita.

L'industria del mining ha diverse economie di scala, a causa di costi energetici, costi di capitale, leggi e normative e complessità della Proof-of-Work. Pertanto, i miner mettono in comune le loro risorse e dividono i premi. Le mining pool consentono ai miner più piccoli di attenuare i loro rendimenti e ridurre il rischio invece di estrarre per rendimenti molto rari ed esorbitanti. Quando un membro di un pool trova un blocco valido, divide i premi con il resto del pool in base al contributo di hashrate di ciascun membro. Gli operatori di mining pool in genere riscuotono una commissione per i loro servizi di coordinamento.

Le pool possono includere centinaia o migliaia di miner, i quali ricevono la loro parte di premio in base alla rispettiva potenza di calcolo offerta. La rete percepisce questi pool come un singolo miner che ha come potenza di calcolo la somma di quella dei suoi partecipanti: in realtà si tratta di un server principale che distribuisce compiti ai singoli miner.

Un pool può supportare la funzione di "difficoltà di condivisione variabile", il che significa che un miner può selezionare da solo l'obiettivo di condivisione (il limite inferiore della difficoltà di condivisione) e modificare la probabilità di trovare un blocco in un tentativo di condivisione di conseguenza.

La lista dei pool per il mining è lunga: nel mondo ce ne sono più di mille. La stragrande maggioranza degli utenti lavora tramite pool di bitcoin. Il livello di complessità della produzione di questa moneta è così alto che da solo, anche con un supercomputer, non si ottiene profitto.

Esistono numerosi sistemi di pagamento applicati dalle mining pool, ma la maggior parte opera con le tipologie di pagamento:

- PPS Pay-Per-Share e PPS+
- FPPS Full Pay Per Share
- PPLNS Pay-Per-Last-N-Shares

Il protocollo usato per fare il mining in pool è Stratum.

Miniscript

Livello: avanzato

Argomento: tecnologia

Miniscript può essere considerato un framework (o template) per Bitcoin Script, il linguaggio di programmazione nativo di Bitcoin. Non è un linguaggio che

sostituisce Bitcoin Script e che chiede quindi aggiornamenti al protocollo o ai nodi, ma un modo diverso di scrivere gli script che viene poi trasformato in Bitcoin Script.

Bitcoin Script consente di creare tutte le condizioni di spesa e degli smart contract Bitcoin, tra cui, ad esempio, quella che forse è la più semplice: determinare chi è autorizzato a spendere un determinato importo Bitcoin.

Per ogni transazione Bitcoin, il mittente richiede l'indirizzo del destinatario e con queste informazioni costruisce uno script che blocca i bitcoin inviati in modo che solo il destinatario possa spenderli. Sebbene sia abbastanza facile costruire script semplici come quello sopra descritto con Bitcoin Script, più lo script diventa complesso, maggiore è la possibilità di errore umano.

Bitcoin Script è un linguaggio stack-based (come il Forth), progettato per implementare condizioni di spesa costituite da varie combinazioni di firme, hash lock e time lock. Tuttavia, nonostante le sue funzionalità limitate, non è affatto banale fare degli script che gestiscano casi come questi:

- Data una combinazione di condizioni di spesa, trovare lo script più economico per implementarla.
- Dati due script, costruire uno script che implementi una composizione delle loro condizioni di spesa (ad esempio un multisig dove una delle "chiavi" è un altro multisig).
- Dato uno script, scoprire quali condizioni di spesa consente.
- Dato uno script e l'accesso a un insieme sufficiente di chiavi private, costruire un testimone generale soddisfacente per esso.
- Dato uno script, essere in grado di prevedere il costo di spesa di un output.
- Dato uno script, sapere se particolari limitazioni di risorse, come il limite di operazioni, potrebbero essere raggiunte durante la spesa.

Miniscript è una rappresentazione degli script che rende più semplice implementare questo tipo di operazioni.

Miniscript consente di scrivere un sottoinsieme di script Bitcoin in modo strutturato. Consente, tra l'altro, l'analisi, la composizione e la firma generica, permettendo agli sviluppatori di scrivere script avanzati in modo più sicuro. In altre parole, Miniscript "contiene" alcune funzionalità degli script Bitcoin preimpostati in base a un modello di comportamento previsto, limitando eventuali rischi in quanto il comportamento inatteso è ridotto al minimo. In pratica, fornisce agli sviluppatori una "cassetta degli attrezzi" per armeggiare e creare script avanzati e complessi per Bitcoin, invece di dover fare tutto manualmente attraverso Bitcoin Script.

Miniscript è stato progettato per gli script embedded P2WSH e P2SH-P2WSH. La maggior parte delle sue costruzioni funziona bene anche in P2SH, ma alcune delle proprietà di sicurezza (opzionali) si basano su regole specifiche di Segwit. Inoltre, i compilatori di policy implementati assumono un modello di costi specifico per Segwit.

A ottobre 2023 è stata aggiunta al codice di Bitcoin Core l'opzione miniscript per i descrittori di output P2TR, Taproot.

un'opzione , aggiungendo il supporto sia per guardare che per firmare i "descrittori TapMiniscript". In precedenza, miniscript era disponibile solo per i descrittori di output P2WSH. L'autore nota che un nuovo frammento multi_a viene introdotto esclusivamente per i descrittori P2TR che corrisponde alla semantica di multi nei descrittori P2WSH. La discussione sul PR rileva che la maggior parte del lavoro è stata finalizzata al corretto monitoraggio dei limiti modificati delle risorse per tapscript.

Miniscript consente al software di analizzare automaticamente uno script, determinando anche quali witness data devono essere generati per spendere i bitcoin protetti da quello script. Con miniscript che dice al wallet cosa deve fare, gli sviluppatori di wallet non devono scrivere nuovo codice quando passano da un modello di script a un altro.

La rappresentazione strutturata degli script Bitcoin fornita da miniscript consente ai wallet di essere molto più dinamici riguardo agli script che utilizzano. A sostegno di questa dinamicità, i miniscript possono essere creati utilizzando un linguaggio di policy di facile scrittura. Le politiche sono componibili, consentendo a qualsiasi sottoespressione valida di essere sostituita da un'altra sottoespressione valida (entro certi limiti imposti dal sistema Bitcoin).

Per esempio lo script Bitcoin:

```
<A> OP_CHECKSIG OP_IFDUP OP_NOTIF OP_DUP OP_HASH160 <hash160(B)>
OP_EQUALVERIFY OP_CHECKSIGVERIFY <144> OP_CSV OP_ENDIF
```

dove A e B sono le chiavi pubbliche, può essere convertito nella notazione Miniscript come:

```
or_d(c:pk(A),and_v(vc:pk_h(B),older(144)))
```

con una notazione che rende chiaro che lo script consente la spesa o quando A firma, o quando B firma dopo 144 blocchi.

Bitcoin Core a partire dalla versione 24.0, consente agli utenti di creare un wallet contenente uno script Miniscript, creare indirizzi per quel wallet e finanziarli con bitcoin. Tuttavia, la spesa da questi indirizzi non è ancora supportata dal wallet di Bitcoin Core, il che significa che i wallet abilitati a Miniscript su Bitcoin Core sono per il momento solo del tipo watch-only.
A ottobre 2023 è stata aggiunta al codice di Bitcoin Core l'opzione per i descrittori di output P2TR, aggiungendo il supporto sia per guardare che per firmare i "descrittori TapMiniscript". In precedenza, miniscript era disponibile solo per i descrittori di output P2WSH. Un nuovo frammento `multi_a` viene introdotto esclusivamente per i descrittori P2TR che corrisponde alla semantica `multi` nei descrittori P2WSH.

minRelayTxFee

Livello: avanzato

Argomento: tecnologia

Il valore minRelayTxFee, definito anche come *Default minimum transaction relay feerates*, specifica un feerate che funge da limite inferiore per la mempool di un nodo. Un nodo non ammetterà transazioni non confermate al di sotto di tale feerate nella sua mempool e quindi non le trasmetterà ai suoi peer. Il minRelayTxFee è un'impostazione di configurazione e può essere specificato da ciascun operatore di nodo in modo indipendente. Il valore influisce solo sulle transazioni non confermate, le transazioni incluse in un blocco vengono elaborate anche se non soddisfano il minRelayTxFee.
Si noti che, contrariamente a quanto suggerisce il nome, il minRelayTxFee non è una fee assoluta, ma un rapporto che stabilisce un valore delle fee sulla dimensione della transazione.

L'attuale valore predefinito per la minRelayTxFee in Bitcoin Core è 1 satoshi per vbyte. L'operatore di un nodo può specificare un valore diverso tramite il parametro di avvio -minrelaytxfee o il parametro di configurazione *minrelaytxfee*. Bitcoin Core trasmette solo transazioni individuali non confermate che pagano un feerate uguale o superiore al minRelayTxFee. Se la mempool di un nodo si riempie di transazioni che pagano almeno 1 sat/vbyte, sarà necessario pagare un feerate più alto. Le transazioni che pagano un feerate inferiore possono comunque essere incluse nei blocchi dai miner e tali blocchi saranno trasmessi. Altri software dei nodi implementano politiche simili. L'abbassamento del feerate minimo predefinito è stato discusso in passato ma non è stato inserito in Bitcoin Core.

La minRelayTxFee serve anche come base per calcolare gli incrementi minimi di costo per le transazioni sostitutive secondo BIP-125 (Opt-in RBF). In precedenza veniva utilizzato anche per calcolare il limite della dust, che da allora è stato disaccoppiato in un feerate separato chiamato DUST_RELAY_TX_FEE con un valore predefinito di 3000 sat/kvB.

minRelayTxFee non deve essere confuso con:

- minTxFee, che è un'impostazione di configurazione del wallet che stabilisce un limite inferiore per la creazione di nuove transazioni
- mempoolminfee, che è un limite inferiore indipendente per l'accettazione del mempool che aumenta dinamicamente quando il limite del mempool viene superato.

Bitcoin Core 0.13.0 ha introdotto un nuovo messaggio P2P opzionale di feefilter, che indica ai nodi vicini di non inviare transazioni al di sotto del feerate del filtro. I nodi più vecchi non comunicano il loro feerate minimo, ma si limitano a eliminare le transazioni in arrivo che non lo superano.

È possibile recuperare i valori correnti per il proprio nodo chiamando l'RPC

getmempoolinfo.

Mint

Coniare

Livello: intermedio

Argomento: tecnologia

Mint, o minting, tradotto letteralmente coniare ma spesso usato con l'inglesismo "mintare", è il processo di generazione di nuovi coin o token (fungibili o NFT) in una blockchain. L'operazione viene effettuata da nodi validatori (nei sistemi che contengono questo tipo di nodi). Nel caso degli NFT, un elemento esposto su un marketplace deve essere mintato per essere venduto, e quindi essere creato nella blockchain per poter essere trasferito dal wallet del creatore a quello dell'acquirente

minTxFee

Livello: avanzato

Argomento: tecnologia

mintxfee è un parametro che significa Minimum Transaction Fee, è un'impostazione di configurazione del wallet che stabilisce un limite inferiore delle fee per la creazione di nuove transazioni.

Il mintxfee, che sta per "Minimum Transaction Fee" (fee minima di transazione), è un parametro di configurazione presente in alcuni wallet Bitcoin, che permette agli utenti di impostare un limite inferiore per le tariffe da pagare per la creazione di nuove transazioni.

In pratica, quando si crea una transazione, il mittente deve pagare una fee ai miner della rete che elaboreranno la transazione e la includeranno nella blockchain. Questa fee viene calcolata in base alla dimensione della transazione e alla domanda di transazioni sulla rete. Il mintxfee consente agli utenti di garantire che le loro transazioni vengano elaborati in modo tempestivo, stabilendo una fee minima da pagare.

Ad esempio, se un utente imposta il mintxfee su 10 satoshi per byte, significa che la fee minima per ogni byte di dati nella transazione sarà di 10 satoshi. Se la dimensione della transazione è di 500 byte, la fee minima totale sarebbe di 5.000 satoshi. Se l'utente tenta di creare una transazione con una fee inferiore al mintxfee impostato, il wallet potrebbe impedire la creazione della transazione o richiedere all'utente di aumentare la fee.

In generale, il mintxfee è una funzionalità utile per gli utenti che desiderano garantire che le loro transazioni vengano elaborate in modo tempestivo e per

evitare di pagare tariffe eccessivamente basse che potrebbero causare un ritardo nell'elaborazione della transazione.

Mixing Service

Livello: avanzato

Argomento: tecnologia

Un mixing service, o più brevemente mixer, conosciuto anche come Tumbler, è un servizio per migliorare la privacy e l'anonimato delle transazioni di criptovaluta mescolando le criptovalute potenzialmente identificabili o "contaminate" con altre transazioni non correlate, rendendo più difficile rintracciare per quale criptovaluta è stata utilizzata e a chi appartiene.

Il mixer consente agli utenti di "offuscare" l'origine e la destinazione delle transazioni: un utente può inviare il quantitativo di bitcoin (o token o altre cripto a seconda del tipo di servizio) di cui ha disponibilità alla piattaforma, la quale mixa o mescola la somma inviata con quella di altri utenti, inviando poi la quantità equivalente all'indirizzo di un destinatario, nascondendo così la connessione con il mittente.

È importante notare che i mixing service non danno una assoluta garanzia di anonimato. È possibile che le autorità governative o altri soggetti anche privati come società di chain analysis siano in grado effettuare analisi e ottenere informazioni sui fondi che sono stati mixati.
Questo può essere fatto utilizzando una serie di tecniche, tra cui l'analisi forense delle transazioni, l'analisi del comportamento degli utenti e la cooperazione con le autorità straniere.

Nella maggior parte dei paesi non esiste una legge che rende illegale l'uso dei tumbler di per se, ma può essere illegale il fatto di usarli per compiere crimini o attività illegali quali il riciclaggio di denaro.

Ad esempio il Dipartimento del Tesoro degli Stati Uniti ha di fatto vietato per tutti i cittadini americani l'utilizzo di Tornado Cash, una delle principali piattaforme di mixing attiva nell'ecosistema Ethereum.
Alexey Pertsev e Roman Storm, fondatori e sviluppatori di Tornado Cash, sono stati arrestati dalle autorità olandesi e americane, con varie accuse tra cui riciclaggio di denaro.
L'OFAC ha inserito in una lista di proscrizione diversi indirizzi riconducibili ad attività con Tornado Cash e gli exchange di criptovalute sono tenuti a bloccare qualsiasi transazione che coinvolga indirizzi critpo inseriti nella lista di proscrizione. Ciò significa che gli utenti che tentano di depositare o prelevare fondi da un exchange utilizzando uno di questi indirizzi saranno bloccati.

Rischio di frode: I mixer bitcoin sono spesso soggetti a frodi. Gli utenti devono prestare attenzione ai mixer bitcoin che non sono affidabili o che potrebbero essere utilizzati per truffare gli utenti.

Mnemonic Wordlist

Frase Mnemonica

Livello: intermedio

Argomento: tecnologia

La Mnemonic Wordlist, o Frase Mnemonica, è un sistema standardizzato introdotto dal BIP 39 nel 2013, che consente di rappresentare una chiave privata di Bitcoin (o di altre criptovalute) attraverso una sequenza di parole di uso comune. Questo metodo rende notevolmente più semplice per gli utenti memorizzare e trascrivere le proprie chiavi private rispetto alle complesse stringhe alfanumeriche tradizionali.

Funzionamento e Vantaggi:

- **Facilità di Memorizzazione**: La frase mnemonica è composta da un elenco di 12, 18 o 24 parole prese da un vocabolario standardizzato (la wordlist BIP39), rendendo il processo di memorizzazione molto più intuitivo rispetto a lunghe sequenze di caratteri casuali.
- **Backup e Recupero**: In caso di smarrimento o danneggiamento del wallet digitale, la frase mnemonica permette di recuperare l'accesso ai propri fondi.
- **Interoperabilità**: Grazie allo standard BIP39, la maggior parte dei wallet Bitcoin e di altre criptovalute supporta l'importazione e l'esportazione di chiavi private tramite frasi mnemoniche, garantendo una buona compatibilità tra diverse piattaforme.

Aspetti Importanti:

- **Derivation Path** (Percorso di Derivazione): Per utilizzare la stessa frase mnemonica su wallet diversi, è fondamentale conoscere il Derivation Path. Questo percorso determina come le chiavi vengono generate dalla frase mnemonica, e variazioni nel percorso possono portare a indirizzi Bitcoin diversi.
- **Sicurezza**: La frase mnemonica rappresenta l'accesso completo ai propri fondi, pertanto è essenziale conservarla in un luogo sicuro e riservato, al riparo da sguardi indiscreti e da potenziali minacce informatiche.
- **BIP39 Wordlist**: La lista di parole usate è standardizzata, ed è importante assicurarsi che nel momento del recupero le parole vengano inserite nello stesso identico ordine.
- **Passphrase opzionale**: Il BIP39 consente di aggiungere una passphrase personalizzata alla frase mnemonica, fungendo da ulteriore livello di sicurezza. L'uso della passphrase rende impossibile accedere ai fondi senza la conoscenza di entrambi i dati.

In sintesi, la Mnemonic Wordlist è uno strumento fondamentale per la gestione sicura e conveniente delle chiavi private nel mondo delle criptovalute.

Money

Denaro

Livello: base

Argomento: economia

Il denaro, in inglese money, o moneta o anche soldi secondo le scienze economiche è uno strumento che può assumere le funzioni di:

- mezzo di scambio
- unità di conto
- riserva di valore
- riferimento per pagamenti dilazionati

Il fatto che Bitcoin e altre criptovalute possano essere considerati denaro è un concetto dibattuto e controverso.
Mentre alcuni sostengono che bitcoin possiede le caratteristiche fondamentali del denaro, come:

- fungibilità,
- divisibilità,
- scarsità
- e accettazione come mezzo di scambio

altri ritengono che manchi di alcune qualità essenziali per essere definito denaro.

Uno degli argomenti a favore del bitcoin come denaro è il suo ruolo come mezzo di scambio digitale.
Le transazioni in bitcoin possono essere eseguite rapidamente e in modo relativamente economico, indipendentemente dalle frontiere geografiche. Inoltre, l'adozione del bitcoin come forma di pagamento è aumentata nel corso degli anni, con diverse aziende e negozi che accettano la criptovaluta come mezzo di pagamento valido. Questo sostiene l'idea che il bitcoin sia una forma di denaro funzionale.

Tuttavia, ci sono alcuni che mettono in discussione che bitcoin possa essere considerato denaro.
Una delle principali critiche riguarda la sua volatilità. Il valore del bitcoin è notoriamente instabile, con oscillazioni di prezzo significative nel corso del tempo.
Questo può rendere difficile l'utilizzo del bitcoin come unità di conto affidabile, poiché il suo valore può fluttuare rapidamente rispetto alle valute fiat che pur avendo nel lungo periodo una inflazione più alta, nel breve periodo hanno un valore più stabile.

In relazione all'incremento dell'offerta monetaria, che può essere causa di inflazione, si parla di bitcoin come hard money. Il concetto di hard money si riferisce a una forma di denaro che è scarsa, limitata nella quantità e difficile da produrre rispetto alle valute fiat, che sono considerate Easy money poiché possono essere create dalle rispettive banche centrali e governi a loro discrezione.

Alcuni considerano che il bitcoin possa essere considerato più come uno store of value o riserva di valore e anche chiamato a questo proposito Oro digitale, piuttosto che come denaro. Questo punto di vista si basa su alcune caratteristiche uniche di bitcoin che lo distinguono come asset di investimento a lungo termine, piuttosto che come mezzo di scambio quotidiano.

Moore's Law

Legge di Moore

Livello: intermedio

Argomento: tecnologia

La legge di Moore ipotizza che il numero di transistor nei circuiti elettronici raddoppia circa ogni due anni.
Questo si traduce approssimativamente in un raddoppio della potenza di elaborazione nello stesso arco temporale.

La legge di Moore è un'osservazione e una proiezione di una tendenza storica.

La legge di Moore non è una legge della fisica o della matematica, ma un'osservazione del rapido ritmo dell'innovazione elettronica.
Sin dagli anni '60, quando è stata proposta la legge di Moore, la tecnologia del mondo reale ha seguito da vicino le previsioni di Moore, portando a una crescita incredibile nell'industria dell'elettronica.

La legge di Moore afferma che le capacità dell'hardware miglioreranno in modo esponenziale. Questi progressi consentono lo sviluppo e l'implementazione di software sempre più ampi, complessi e intensivi senza esaurire le capacità dell'hardware disponibile.

In assenza del rapido tasso di innovazione, non saremmo in grado di eseguire programmi intensivi di apprendimento automatico, intelligenza artificiale o mining di Bitcoin su cui si basano Bitcoin e altre industrie ad alta tecnologia.

Nel Whitepaper Bitcoin viene citata la legge di Moore nel seguente passaggio:

Dato che nel 2008 sono in vendita computer con circa 2GB di RAM, e la Legge di Moore predice una crescita di 1.2GB per anno, lo spazio di archiviazione non dovrebbe rappresentare un problema anche se le intestazioni dei blocchi devono essere immagazzinate in memoria.

in relazione alla necessità di memoria per conservare la block chain.

MPC

Acronimo di: Multi-Party Computation

Livello: avanzato

Argomento: tecnologia

Il Multi-Party Computation, noto anche come MPC o Secure MPC (SMPC), funziona come un protocollo che facilita la risoluzione collaborativa di questioni riservate.
Svolge un ruolo cruciale nel garantire la privacy in un ambiente in cui la conservazione dei dati riservati, in particolare online, pone sfide significative.

Nel caso di Bitcoin, l'MPC può essere utilizzato per la creazione di wallet MPC. Un wallet MPC è un tipo di wallet di criptovalute che utilizza la tecnologia MPC per dividere e distribuire le chiavi private tra più parti in modo sicuro. Questo rende più difficile per un attore malintenzionato ottenere l'accesso a tutte le chiavi e quindi ai fondi dell'utente.

Il funzionamento di un wallet MPC è il seguente:

1. L'utente genera un seed segreto, che viene poi suddiviso in più frammenti.

- Ogni frammento viene distribuito a una parte diversa, che può essere una persona, un'organizzazione o un dispositivo.
- Per inviare una transazione, l'utente deve collaborare con le altre parti per combinare i loro frammenti e creare una firma valida.

Nel caso di Bitcoin, la tecnologia MPC può essere utilizzata per creare dei MPC wallet, che in generale funziona in questo modo:

1. Le parti che condividono i frammenti della chiave privata utilizzano un protocollo MPC per elaborare le informazioni in modo sicuro.

- Il protocollo MPC garantisce che nessuna parte possa accedere o modificare le informazioni senza il consenso delle altre parti.

I MPC wallet offrono diversi vantaggi rispetto ai wallet tradizionali:

- Migliore sicurezza: la distribuzione delle chiavi private tra più parti rende più difficile per un attore malintenzionato ottenere l'accesso ai fondi dell'utente.
- Riduzione del rischio di frodi: i MPC wallet possono aiutare a ridurre il rischio di frodi, come l'appropriazione indebita di fondi o l'hacking.
- Maggiore flessibilità: i MPC wallet possono essere utilizzati per creare diversi tipi di configurazioni di sicurezza, ad esempio per consentire a più persone di accedere ai fondi di un wallet.

Tuttavia, i MPC wallet presentano anche alcuni svantaggi rispetto ai normali wallet:

- Maggiore complessità: la tecnologia MPC è complessa e può essere difficile da comprendere.
- Maggiori costi: i MPC wallet possono essere più costosi dei wallet tradizionali.

Differenze tra wallet MPC e multisig Sebbene sia vero che l'intento principale dietro la creazione di wallet MPC e multisig fosse in entrambi i casi quello di aumentare la privacy e rafforzare la sicurezza, il modus operandi di questi due tipi di wallet è diverso. I meccanismi con cui funzionano sono intrinsecamente diversi, nonostante abbiano alcune apparenti somiglianze nei loro scopi.

I meccanismi dei wallet multisig Un wallet multisig funziona inviando transazioni blockchain attraverso un componente di identificazione univoco: una firma. Affinché una transazione venga autenticata e finalizzata all'interno di questo wallet, è necessario che siano convalidate almeno due chiavi private. In sostanza, ciascuna parte coinvolta nella transazione è tenuta a fornire una chiave privata come mezzo di approvazione.

Comprendere la funzionalità dei wallet MPC D'altro canto, i wallet MPC adottano un approccio diverso disperdendo un'unica chiave privata tra più parti. Questo metodo rende l'interazione più snella e meno complicata, migliorando l'esperienza dell'utente mantenendo elevati livelli di sicurezza.

Nonostante le somiglianze nello scopo, le complessità tecniche di questi wallet li distinguono. I wallet MPC offrono maggiore flessibilità e sono generalmente più semplici da utilizzare e implementare. Ciò non solo riduce la necessità di più chiavi private, ma migliora anche significativamente la comodità dell'utente senza compromettere la sicurezza delle transazioni. Una comprensione approfondita di queste differenze è essenziale per scegliere il wallet giusto per le esigenze individuali o aziendali.

Come soluzione intermedia ideale, i wallet MPC stanno guadagnando popolarità grazie alla loro capacità di offrire una potente combinazione di maggiore sicurezza e comodità. In sostanza, questi wallet riducono o alleviano i problemi comunemente associati ai tradizionali tipi di wallet.

In sostanza, l'utilizzo dei wallet MPC veicola:

- Misure di sicurezza amplificate
- Maggiore livello di comodità per l'utente
- Rischi mitigati prevalenti in altri tipi di wallet

Comprendere gli svantaggi dei wallet MPC È fondamentale analizzare non solo i vantaggi ma anche i potenziali svantaggi legati all'uso dei wallet MPC (Multi-Party Computation). A prima vista, questi wallet digitali promettono misure di sicurezza avanzate e un'efficace gestione delle risorse crittografiche. Tuttavia non sono privi di insidie, che gli utenti devono comprendere a fondo

prima di optare per questa forma di archiviazione di risorse digitali.
Tra i rischi associati all'uso dei wallet MPC è vitale per un processo decisionale informato. Questi archivi digitali, nonostante i loro vantaggi, comportano numerosi rischi.

Picco di complessità Per cominciare, i wallet MPC hanno una configurazione operativa più complessa rispetto ai wallet tradizionali. Questa complessità deriva dal meccanismo di crittografia che, sebbene progettato per fornire sicurezza rafforzata, può essere un deterrente per gli utenti non esperti. Inoltre, il tracciamento di una transazione, in caso di problemi, può essere piuttosto impegnativo a causa di questo sistema complesso.

Maggiore vulnerabilità In secondo luogo, potrebbe esserci un aumento del rischio di esposizione ad attacchi informatici a causa delle complessità coinvolte nella configurazione funzionale di un wallet MPC. Nonostante le loro funzionalità di sicurezza avanzate, questi wallet possono ancora essere il bersaglio degli hacker che mirano a sfruttare ogni possibile vulnerabilità.

Dipendenza da partecipanti aggiuntivi Un altro inconveniente risiede nel coinvolgimento di più parti necessario affinché qualsiasi transazione abbia successo. Il processo richiede il consenso di ciascuna delle parti, il che porta alla dipendenza e quindi a un potenziale rallentamento o cessazione della transazione in caso di disaccordo.

Familiarizzando con queste potenziali sfide o inconvenienti, gli utenti possono prendere decisioni più informate riguardo all'uso dei wallet MPC per la gestione delle risorse digitali. Sebbene forniscano funzionalità di sicurezza all'avanguardia, gli individui devono anche essere preparati ad affrontare le complessità intrinseche e le potenziali vulnerabilità.

Applicazioni pratiche del wallet MPC La tecnologia Secure Multi-Party Computation (MPC) è rapidamente emersa come la soluzione di sicurezza preferita tra le organizzazioni su larga scala, grazie ai suoi numerosi vantaggi. Gli istituti finanziari riconosciuti hanno gradualmente integrato MPC nelle loro operazioni principali, rafforzando le proprie risorse contro violazioni della sicurezza sia interne che esterne.

Lo spostamento verso i wallet MPC Di fronte alle crescenti minacce alla sicurezza informatica, le entità finanziarie trovano sempre più conforto nell'adozione dei wallet MPC. Guidati dai vantaggi intrinseci della tecnologia MPC per la protezione patrimoniale, le banche e gli istituti finanziari stanno sfruttando questa innovazione per salvaguardie interne migliori e solide.

MPP

Acronimo di: Multi-Path Payment

Livello: avanzato

Argomento: tecnologia

MPP Multi-Path Payment o Multi Part payments, sono un tipo di pagamento su Lightning Network che viene eseguito come un insieme atomico di pagamenti più piccoli.

Sono una funzionalità che è stata introdotta in Lightning Network nel 2020 e sono già ampiamente disponibili.

Questi pagamenti più piccoli sono più affidabili e più facili da eseguire; offrono anche vantaggi in termini di privacy, in quanto un insieme di pagamenti multipath è più difficile da tracciare di un singolo pagamento.

I pagamenti multipath sono atomici, il che significa che devono avere tutti successo, altrimenti se ne fallisce anche solo uno falliscono tutti: alla fine tutte le parti HTLC di un pagamento vengono soddisfatte o l'intero pagamento fallisce e tutte le parti HTLC falliscono. Non vi è alcuna possibilità di un pagamento parzialmente andato a buon fine.

I pagamenti multipath risolvono alcuni problemi della rete Lightning. Quando viene attivato un canale Lightning, ha una capacità definita. Ogni utente può inviare su questo canale solo tanti bitcoin quanti ne ha impegnati nel canale. Quindi, i pagamenti più grandi della capacità di un canale falliscono se la capacità è insufficiente. Questo problema è particolarmente saliente per i pagamenti instradati (routed payments), che attraversano diversi canali per arrivare dal mittente al ricevitore. Al fine di consentire pagamenti di grandi dimensioni, le implementazioni Lightning permettono agli utenti o ai loro wallet Lightning di suddividere il pagamento in pagamenti più piccoli. Ogni pagamento può essere instradato attraverso un percorso diverso, distribuendo l'impegno su molti canali diversi.

Esistono diverse proposte e implementazioni di questo concetto nelle diverse implementazioni Lightning, tra cui MPP di base e Atomic Multipath Payments (AMP). Queste diverse versioni tentano di risolvere diversi problemi di sicurezza e affidabilità con il concetto di base dei pagamenti multipath.

Zero Base Fee può essere una tecnica che permette di ottimizzare la rete Lightning Network e di aumentarne la velocità e la scalabilità dei pagamenti MPP.

MRI

Acronimo di: Momentum Reversal Indicator

Livello: avanzato

Argomento: finanza

The MRI, Momentum Reversal Indicator o indicatore di inversione del momentum è una metrica avanzata di analisi tecnica che predice i cicli di vita del trend

basandosi sul momentum di un asset.

Il momentum è un concetto chiave nell'analisi tecnica, che si riferisce alla forza di un'azione in una determinata direzione. Gli indicatori di momentum sono strumenti utilizzati dagli investitori per valutare la forza del trend di un'azione e per identificare i possibili punti di inversione.

Gli indicatori di momentum più comuni includono il RSI Relative Strength Index, lo Stochastic Oscillator e il Moving Average Convergence Divergence (MACD). Questi strumenti possono aiutare gli investitori a prendere decisioni di trading informate e a gestire il rischio.

Tuttavia, è importante notare che nessun indicatore di momentum può prevedere con certezza l'andamento futuro del mercato azionario. Gli investitori dovrebbero sempre valutare una serie di fattori, tra cui gli indicatori tecnici, i dati fondamentali dell'azienda e le condizioni del mercato più ampio, prima di prendere una decisione di trading.

MS-SMT

Acronimo di: Merkle-Sum Sparse Merkle tree

Livello: avanzato

Argomento: tecnologia

MS-SMT, acronimo Merkle-Sum Sparse Merkle tree, è una nuova struttura ad albero utilizzata da Taro per migliorare la scalabilità e la privacy dell'emissione e dell'utilizzo delle monete.

Sparse Merkle tree e Merkle-Sum Tree sono combinati per formare Merkle-Sum Sparse Merkle tree.

Merkle-Sum Tree è un tipo di Merkle tree che rende efficiente la verifica dell'assenza di cambiamenti nel valore cumulativo o nella distribuzione delle foglie di un Merkle tree.

Sparse Merkle tree è come un Merkle tree standard, eccetto che i dati contenuti sono indicizzati, e ogni datapoint è posizionato alla foglia che corrisponde all'indice di quel datapoint.

Taro utilizza una combinazione dei concetti sopra descritti per consentire l'emissione di asset nativi su Bitcoin.

MSB

Acronimo di: Money Service Business

Livello: intermedio

Argomento: legale

MSB, acronimo di Money Service Business, è un termine giuridico utilizzato dalle autorità di regolamentazione finanziaria per descrivere le attività che trasmettono o convertono denaro.

Gli MSB devono rispettare regolamenti e normative specifiche, spesso imposte da autorità finanziarie o organizzazioni di regolamentazione, con finalità AML e KYC. In molte giurisdizioni, gli MSB sono tenuti a registrarsi e ottenere una licenza per operare legalmente.

Le normative specifiche possono variare da paese a paese, e talvolta anche all'interno di un singolo paese a seconda delle giurisdizioni locali.

In Italia, le MSB sono disciplinate dalla Legge n. 231 del 2007, che recepisce la Direttiva 2005/60/CE dell'Unione Europea in materia di contrasto al riciclaggio e al finanziamento del terrorismo.

Le MSB possono essere suddivise in due categorie principali:

- **Money transmitter**: si tratta di imprese che si occupano di trasferire denaro da un conto bancario a un altro, o da un paese a un altro. Ad esempio, rientrano in questa categoria le società di money transfer, le banche e le Poste Italiane.
- **Currency dealer or exchanger**: si tratta di imprese che si occupano di convertire valute. Ad esempio, rientrano in questa categoria le società di cambio valuta, le banche e le Poste Italiane.

In Italia, le MSB sono tenute a registrarsi presso la Banca d'Italia, che vigila sul loro operato. Le MSB sono soggette a una serie di obblighi di trasparenza e di contrasto al riciclaggio e al finanziamento del terrorismo, tra cui:

- Obbligo di identificazione dei clienti: le MSB devono identificare i propri clienti, raccogliendo i dati anagrafici, il codice fiscale e, in alcuni casi, anche il documento di identità.
- Obbligo di segnalazione di operazioni sospette: le MSB devono segnalare alla Banca d'Italia le operazioni che presentano elementi di anomalia.

Le MSB che non si conformano agli obblighi di legge possono essere sanzionate dalla Banca d'Italia.

Alcune esempi di MSB in Italia sono: Western Union, MoneyGram, N26, Revolut, TransferWise

Queste imprese offrono una serie di servizi di trasferimento e conversione di denaro, tra cui:

- Trasferimento di denaro da un conto bancario a un altro
- Trasferimento di denaro da un paese a un altro
- Conversione di valute
- Acquisto di carte prepagate
- Ricarica di carte prepagate
- Pagamento di bollette e utenze

Multisig

Acronimo di: Multi-Signature

multi-firma

Livello: intermedio

Argomento: tecnologia

La tecnologia multisig, abbreviazione di multi signature o multi firma, consente a due o più utenti di firmare collettivamente documenti digitali o transazioni in criptovaluta.

Le firme multisig Bitcoin sono un tipo di firma digitale che richiede più di una chiave privata per essere valida. In un normale wallet Bitcoin, una sola chiave privata è sufficiente per autorizzare una transazione. I wallet multisig richiedono invece un numero minimo di firme per eseguire una transazione.

Ad esempio, un wallet 2-of-3 richiede due firme su tre per autorizzare una transazione. Questo significa che due persone o organizzazioni devono firmare la transazione affinché venga eseguita.

Le firme multisig possono essere utilizzate per aumentare la sicurezza dei wallet Bitcoin. Se una chiave privata viene compromessa, le persone o organizzazioni che possiedono le altre chiavi private possono ancora impedire che i fondi vengano rubati.

Le firme multisig possono anche essere utilizzate per decentralizzare il controllo dei fondi Bitcoin. Ad esempio, un'organizzazione potrebbe utilizzare un wallet multisig per distribuire le chiavi private tra diversi membri del team. Ciò impedirebbe a una singola persona o organizzazione di controllare tutti i fondi.

Esistono diversi modi per creare un wallet multisig Bitcoin. Alcuni wallet software, come Electrum e Wasabi Wallet, supportano le firme multisig. È anche possibile creare un wallet multisig utilizzando un servizio di custodia di terze parti.

Ecco un esempio di come funzionano le firme multisig Bitcoin:

- Alice e Bob creano un wallet multisig 2-of-3.
- Alice riceve una chiave privata e Bob riceve due chiavi private.
- Alice e Bob vogliono trasferire 1 BTC da un wallet a un altro.
- Alice firma la transazione con la sua chiave privata.
- Bob firma la transazione con una delle sue chiavi private.
- La transazione viene trasmessa alla rete Bitcoin.
- La rete Bitcoin verifica le firme e approva la transazione.
- I fondi vengono quindi trasferiti dal wallet originale al nuovo wallet.

Le firme multisig sono un modo efficace per aumentare la sicurezza e la decentralizzazione dei wallet Bitcoin.

Poiché gli indirizzi multisig sono hash degli script che contengono le chiavi pubbliche di tutti i partecipanti, anche se in un multisig 2 su 3 hai bisogno di solo 2 chiavi per firmare, l'indirizzo che stai firmando richiede tutte e 3 le chiavi pubbliche, il che significa che è necessario avere un backup delle xpub.

Una alternativa al multisig sono i wallet MPC, o Multi-Party Computation.

MuSig

Livello: avanzato

Argomento: tecnologia

MuSig è un protocollo per la creazione di chiavi pubbliche e firme multisig di Taproot.

MuSig utilizza l'aggregazione di firme e chiavi pubbliche di Schnorr ed è stata resa possibile con l'attivazione dell'aggiornamento di Taproot.

La particolarità di MuSig è che una transazione multisig risultante non è più distinguibile da una transazione a firma singola. Questo perché MuSig combina le singole chiavi pubbliche di ciascuna parte per creare un'unica chiave pubblica. Quando vengono spesi i bitcoin da questa chiave pubblica, i partecipanti non sono costretti a rivelare le loro chiavi pubbliche individuali. Al contrario, creano collettivamente una singola firma valida per la chiave pubblica creata in precedenza. Questo non è il caso delle tipiche transazioni multisig, che utilizzano script P2SH e obbligano a rivelare le firme e le chiavi pubbliche di ciascun firmatario sulla blockchain.

MuSig presenta un significativo miglioramento della privacy rispetto all'attuale implementazione multisig, e non solo per gli utenti MuSig. MuSig metterà in crisi molte euristiche attualmente utilizzate per Chain Analysis, eliminando qualsiasi differenziazione tra transazioni a firma singola e transazioni a firma multipla.

Rispetto alla multisig basata su script tradizionali, MuSig utilizza meno spazio nel blocco ed è più privato, ma richiede anche più interattività tra i partecipanti. Ci sono tre protocolli nella famiglia MuSig:

- MuSig (anche chiamato MuSig1), che dovrebbe essere semplice da implementare ma richiede tre round di comunicazione durante il processo di firma.
- MuSig2, anch'esso semplice da implementare. Elimina un round di comunicazione e consente di combinare un altro round con lo scambio di chiavi. Ciò può consentire di utilizzare un processo di firma abbastanza simile a quello che usiamo oggi con la multisig basata su script. Ciò richiede di archiviare dati aggiuntivi e di essere molto attenti a garantire che il software o l'hardware di firma non possano essere ingannati a ripetere parte della sessione di firma in modo inconsapevole.

- MuSig-DN (Deterministic Nonce), significativamente più complesso da implementare. La sua comunicazione tra i partecipanti non può essere combinata con lo scambio di chiavi, ma ha il vantaggio che non è vulnerabile all'attacco di sessione ripetuta.

Nakamoto Consensus

Consenso di Nakamoto

Livello: intermedio

Argomento: tecnologia

Il Nakamoto Consensus, chiamato anche Consenso di Nakamoto, è un concetto fondamentale nel contesto di Bitcoin e delle criptovalute basate sulla sua tecnologia. È stato introdotto da Satoshi Nakamoto, l'anonimo creatore di Bitcoin.

Il Nakamoto Consensus si riferisce al metodo attraverso il quale viene raggiunta l'accettazione e la validazione delle transazioni all'interno della rete Bitcoin. In sostanza, stabilisce il modo in cui i partecipanti alla rete Bitcoin raggiungono un consenso sullo stato corrente del registro delle transazioni, noto come block chain.

Il consenso di Nakamoto si basa sull'uso del proof-of-work come meccanismo di consenso. I partecipanti della rete, chiamati miner, competono per risolvere una prova crittografica. Il miner che riesce a trovare la prova per primo può proporre un nuovo blocco di transazioni da aggiungere alla block chain. Questo processo richiede una quantità significativa di potenza di calcolo e risorse, rendendolo computazionalmente oneroso. Una volta che il blocco è proposto, gli altri nodi della rete lo convalidano e lo accettano se è conforme alle regole del protocollo Bitcoin.

Il Nakamoto Consensus garantisce la sicurezza e l'integrità del sistema Bitcoin, in quanto richiede che la maggioranza dei partecipanti sia onesta e cooperi secondo le regole del protocollo. In teoria, un attaccante dovrebbe controllare la maggioranza della potenza di calcolo della rete, conosciuta come attacco del 51%, per poter manipolare o alterare le transazioni. Questo rende il sistema Bitcoin sicuro e resistente a manipolazioni da parte di singoli individui o gruppi malevoli.

Nash equilibrium

Equilibrio di Nash

Livello: intermedio

Argomento: politica

L'equilibrio di Nash, a volte indicato come gli equilibri di Cournot-Nash, rappresenta un concetto fondamentale all'interno della teoria dei giochi, un ramo

dell'economia e della matematica che studia il comportamento strategico dei giocatori in situazioni di interazione.
In un contesto di gioco, si verifica un equilibrio di Nash quando ciascun giocatore seleziona la strategia ottimale sulla base delle scelte degli altri partecipanti, senza che vi sia la possibilità di ottenere un miglioramento unilaterale della propria situazione. In altre parole, nessun giocatore ha un incentivo a deviare dalla propria scelta, considerando le scelte degli altri giocatori.

Nel contesto dei Bitcoin, l'equilibrio di Nash può essere correlato al concetto di mining, il processo attraverso il quale vengono creati nuovi Bitcoin e registrate le transazioni nella blockchain. I miner utilizzano enormi capacità di elaborazione per validare i blocchi trovando un codice particolare, e chiunque risolva il problema per primo ottiene una ricompensa in Bitcoin.
Un equilibrio di Nash si verifica quando ogni miner decide di utilizzare la propria capacità computazionale in modo da massimizzare il proprio guadagno con un comportamento onesto, ovvero seguendo le regole del protocollo invece di utilizzarlo per alterare le transazioni. Nessun miner dovrebbe avere l'incentivo ad utilizzare la propria capacità di calcolo per effettuare un attacco, ad esempio l'attacco del 51%.
L'equilibrio di Nash avvantaggia sia i miner onesti che la sicurezza della rete, che a sua volta attira più miner a unirsi alla sua rete.

John Nash è stato anche l'ideatore di una moneta ideale teorica che cercava di rimuovere l'elemento soggettivo dalla macroeconomia e stabilire un indice internazionale stabile che potesse fornire un confronto apolitico affidabile per ogni fiat sovrano.
Questa proposta funziona in modo opposto al modo con cui operano le banche centrali: non offre loro spazio di manovra nella gestione dei propri affari e l'inelasticità di un tale indice rende quasi impossibile mantenere un ancoraggio.
La rimozione dell'inflazione da parte di Nash diventa paragonabile alla rimozione del postulato della mediazione da parte di Satoshi: Bitcoin ha creato una nuova e parallela forma di denaro in cui i mandanti non sono richiesti al momento del regolamento.

Nel gioco non cooperativo, i partecipanti assimilano le mosse in relazione agli altri: gli equilibri si stabilizzano dove non si può ottenere un vantaggio unilaterale dal deviare dalle regole.
Nel gioco macroeconomico monetario, Bitcoin ha creato un nuovo equilibrio tra denaro basato sulla fiducia (la parola del governo o della banca centrale) e quello senza fiducia (basato sulla matematica) e le assimilazioni vengono ancora fatte man mano che il gioco procede.

E con questa linea di pensiero, i primi lavori di Nash sulla contrattazione prima degli equilibri e Ideal Money possono essere visti rilevanti per le osservazioni di Satoshi sulla piccola transazione casuale.

NAT

Acronimo di: Network-adjusted time

Livello: intermedio

Argomento: tecnologia

Il Network-adjusted time (NAT) in Bitcoin è un sistema utilizzato per sincronizzare l'orologio dei nodi della rete Bitcoin.
Poiché Bitcoin è una rete decentralizzata, i nodi possono trovarsi ad avere orologi che mostrano tempi leggermente diversi anche tenendo in considerazione il diverso fuso orario.
Il NAT è progettato per ridurre al minimo il divario temporale tra i nodi, consentendo una migliore sincronizzazione delle transazioni e dei blocchi.

Il NAT funziona calcolando la media ponderata dei tempi segnalati da una selezione di nodi all'interno della rete Bitcoin. Questo fornisce un tempo di riferimento più accurato rispetto all'utilizzo dell'orologio di un singolo nodo. Utilizzando il NAT, i nodi possono quindi regolare i propri orologi per mantenere una migliore coerenza temporale all'interno della rete. Questa sincronizzazione consente un corretto funzionamento della blockchain Bitcoin e per evitare problemi come il "tempo di raddoppio" che potrebbe compromettere la sicurezza della rete.

Dalla versione Bitcoin Core 27.0, rilasciata ad Aprile 2024, viene rimosso Network-adjusted time con la seguente spiegazione:
Network-adjusted time è stato sostituito con l'ora di sistema (unadjusted). Rimane attivo l'avviso in caso di un grande scarto temporale mediano (70 minuti o più).
Questo cambiamento elimina il presupposto di sicurezza implicito che richiedeva una maggioranza onesta di peer in uscita, e aumenta l'importanza per l'operatore del nodo di assicurarsi che la propria ora di sistema sia (e rimanga) corretto per non perdere il consenso con la rete. Questo l'obbiettivo della rimozione:

- Maggiore responsabilità per gli operatori dei nodi: diventa fondamentale assicurarsi che l'ora di sistema sia corretta e rimanga tale, per evitare di perdere il consenso con la rete.
- Minore affidamento all'onestà della maggioranza: in precedenza, anche se alcuni partecipanti avessero inviato informazioni orarie scorrette, il software sarebbe comunque riuscito a correggere l'ora. Ora è più importante che ogni singolo nodo abbia l'ora corretta. Utile ad esempio in caso di eclipse attack

Nested SegWit

Livello: intermedio

Argomento: tecnologia

Un indirizzo Bitcoin di tipo Nested SegWit, indicato anche con il termine Wrapped SegWit, è un indirizzo che utilizza il formato P2SH per implementare un indirizzo di tipo SegWit. Questo significa che l'indirizzo è in grado di gestire transazioni SegWit, ma lo fa in modo compatibile con i wallet Bitcoin legacy.

Gli indirizzi Nested SegWit iniziano con il carattere "3". Il resto dell'indirizzo è un hash della chiave pubblica del destinatario.

Gli indirizzi Nested SegWit offrono diversi vantaggi rispetto agli indirizzi legacy Bitcoin, tra cui:

- Commissioni di transazione più basse: le transazioni SegWit sono più efficienti in termini di spazio, il che consente di includere più transazioni in ogni blocco. Questo può portare a commissioni di transazione più basse.
- Supporto per i wallet legacy: gli indirizzi Nested SegWit sono compatibili con i wallet Bitcoin legacy. Ciò significa che i wallet legacy possono inviare e ricevere fondi da indirizzi Nested SegWit.

Tuttavia, gli indirizzi Nested SegWit non offrono gli stessi vantaggi degli indirizzi SegWit nativi o bech32. Gli indirizzi SegWit nativi sono ancora più efficienti in termini di spazio e offrono commissioni di transazione ancora più basse.

Gli indirizzi Nested SegWit sono stati un compromesso per consentire l'utilizzo di wallet Bitcoin legacy, ma ormai quasi tutti i wallet Bitcoin supportano SegWit nativi e dovrebbero utilizzare indirizzi SegWit nativi per ottenere i migliori vantaggi in termini di prestazioni e costi.

Network

rete

Livello: base

Argomento: tecnologia

Un network, o rete, si riferisce a un insieme nodi tra di loro interconnessi.

Un nodo è un membro discreto di una rete che interagisce con altri nodi per formare la rete, e questi nodi comunicano tra di loro secondo le regole stabilite dal protocollo al quale i nodi aderiscono, questo protocollo è un insieme di regole e politiche che vengono decise per consentire la partecipazione alla rete.
Queste politiche configurano non solo le modalità con cui i nodi si scambiano le informazioni, ma anche elementi cruciali della rete, come il meccanismo di consenso.

Nel caso di Bitcoin, la tipologia di rete è quella di tipo p2p, o peer to peer, nella quale il rapporto tra i vari nodi ai fini della distribuzione delle informazioni viene considerato paritetico. È un sistema distribuito e decentralizzato che non è controllato da alcuna autorità centrale. Ciò consente che i bitcoin non possono essere censurati o bloccati da governi o istituzioni finanziarie.

La rete Bitcoin è una rete di pagamento peer-to-peer che opera su un protocollo crittografico.

I nodi convalidano, diffondono e richiedono transazioni, blocchi e la mempool da e verso i propri pari nella rete.
Se i nodi eseguono software compatibili, si raggiunge il consenso.

Gli utenti inviano e ricevono bitcoin, le unità di valuta, diffondendo messaggi digitalmente firmati alla rete utilizzando il software dei wallet. Questi messaggi contengono le transazioni che vengono registrate in un database pubblico distribuito e replicato noto come blockchain, con il consenso raggiunto attraverso un sistema di proof-of-work chiamato mining.

La rete bitcoin è decentralizzata ed è formata da utenti volontari, e con network si intende tutti i nodi che partecipano in un dato momento nel tempo, i nodi possono abbandonare e rientrare nella rete a loro piacimento.

Al momento del riconnessione, un nodo scarica e verifica nuovi blocchi da altri nodi per completare la propria copia locale della blockchain.

La rete Bitcoin è la più resistente, affidabile e resiliente poiché dal suo avvio il 3 gennaio 2009 si è fermata solo due volte nella sua storia, e ha un uptime del 99,98%.
Il termine inglese uptime (letteralmente tempo in attività, traducibile in tempo di funzionamento) denota l'intervallo di tempo in cui un singolo apparato o un intero sistema informatico è stato ininterrottamente acceso e correttamente funzionante. Il termine opposto, downtime (traducibile in tempo di inattività) , denota lo stato di un sistema che non è operativo oppure l'intervallo di tempo in cui un sistema è in tale stato, che può essere dovuto ad un guasto, a manutenzione o altre cause.

NFA

Acronimo di: Not financial advice

Non è un consiglio finanziario

Livello: intermedio

Argomento: legale

Frase che viene detta spesso proprio da chi i consigli finanziari li ha appena dati o li sta per dare, ma non avendone titolo legale per farlo usa questa formula nella speranza di evitarne le conseguenze.

Le vostre opinioni personali su ciò che "nessuno sano di mente" farebbe o non farebbe non sono legge. A seconda del luogo in cui si vive, esistono numerose leggi e regolamenti che disciplinano determinati tipi di consulenza.

Ad esempio nell'Unione Europea il MiCA, il disegno di legge sui mercati degli asset crittografici approvato dalla Commissione per gli affari economici e monetari

del Parlamento europeo il 10 ottobre 2022, contiene una sezione che potrebbe avere un impatto su molti commentatori o influencer di criptovalute: commentare gli asset crittografici su social media senza divulgazione e trarre profitto dagli effetti di ciò sarà considerato manipolazione del mercato nell'UE una volta che il MiCA sarà operativo.

Alcune consulenze sono sufficientemente specializzate da permettere alle persone di affidarsi a esse per questioni di vita o di morte; in queste aree tematiche si applicano pene significative a coloro che le forniscono per negligenza. Le aree tematiche specifiche, le licenze coinvolte e le pene dipendono dalla giurisdizione in cui ci si trova, ma in tutto il mondo sono molto reali.

Immaginate di vivere in un luogo in cui i meccanici che vi dicono "oh, devi ripararlo subito" quando in realtà non è necessario, potrebbero essere citati in giudizio, o i meccanici che vi dicono "puoi lasciarlo così per qualche mese" ma poi avete un incidente, potrebbero essere citati in giudizio.

(In questo mondo, i meccanici sarebbero molto cauti nel dare consigli sulle auto. Il vostro vicino di casa potrebbe ancora dire "oh, a noi è successo con la nostra auto e abbiamo aspettato 6 mesi per ripararla, nessun problema" perché sapreste che il vostro vicino non è un meccanico autorizzato e quindi non sta dando ciò che si qualifica legalmente come consulenza automobilistica, ma solo condividendo un'opinione.

Quando si guarda un video su YouTube, si legge un blog o un articolo su una rivista, non è scontato su quanto possiamo affidarci ai consigli che vengono espressi. Queste persone vi stanno dando ciò che si qualifica legalmente come consulenza tematica (che sia medica, finanziaria, legale o altro) o sta solo condividendo la sua opinione? Se vi sta dando una consulenza tematica, potrebbe rischiare la licenza, le multe, la denuncia e persino il carcere se lo fa in modo ingannevole, negligente, sconsiderato e così via. E se non hanno una licenza da rischiare, ci sono sanzioni per chi fa cose che richiedono una licenza senza averla. Se stanno solo condividendo un'opinione, non ce l'hanno.

Di conseguenza, le persone che hanno una licenza da perdere (e sì, ci sono licenze e simili legate all'essere un consulente finanziario) o che potrebbero apparire come tali, rilasceranno una dichiarazione di non responsabilità per il fatto che ciò che stanno dicendo è solo la loro opinione casuale in generale e non un consiglio specifico per la vostra situazione su cui potete fare affidamento in senso normativo.

A volte questa dichiarazione di non responsabilità è priva di significato.

Se qualcuno vi dice quali sono i sintomi di un ictus e cosa fare in caso di ictus, non direte in seguito "Non lo so, in quel video c'era scritto di chiamare il 911, ma hanno detto che non era un consiglio medico". Ma spesso questo disclaimer è molto utile.

Questa persona mi parla di Bitcoin o di qualche azione di cui non ho mai sentito parlare o di qualche borsa valori di cui non ho mai sentito parlare, assicurandomi

che se seguirò il suo consiglio non gli costerà mai nulla.

NFC Unicode

Acronimo di: Normalization Form C

Forma di normalizzazione C di Unicode

Livello: avanzato

Argomento: tecnologia

NFC in Unicode (Normalization Form Canonical Composition) è uno standard che assicura che le stringhe di testo Unicode equivalenti abbiano la stessa rappresentazione binaria. In pratica, converte le diverse sequenze di caratteri Unicode che producono lo stesso glifo in una forma standard unica.

Bitcoin nel BIP-38 utilizza NFC Unicode per la passpharse.

NFKD

Acronimo di: Normalization Form Compatibility Decomposition

Forma di Normalizzazione con Decomposizione di Compatibilità Unicode

Livello: avanzato

Argomento: tecnologia

Lo standard Unicode per la rappresentazione dei caratteri nelle varie lingue ha diverse modalità per rappresentare gli stessi caratteri.

Una di queste è la NFKD, che è stata scelta per rappresentare la passphrase del BIP-39.

L'uso di certi caratteri speciali o accentati nella passphrase può portare a problemi di compatibilità tra wallet o, nei casi peggiori, all'impossibilità di recuperare i fondi.
Questo perché con l'NFKD caratteri che sono rappresentati visivamente identici, possono essere codificati diversamente e non vengono riconosciuti.

NFT

Acronimo di: Non Fungible Token

Token non fungibili

Livello: base

Argomento: tecnologia

La fungibilità è la proprietà di un bene o una risorsa di essere rappresentabile per il suo valore e conseguentemente essere intercambiabile.

Ad esempio 1 Bitcoin ha lo stesso valore di 1 altro Bitcoin, 10 monete da 1 euro sono intercambiabili con 1 banconota da 10 euro.

Gli NFT (non-fungible token, Token Non Fungibili) sono dei token che non possono essere rappresentati solo per il loro valore, poiché hanno delle caratteristiche che li rendono unici. Nel settore delle criptovalute gli NFT possono essere utilizzati come dei titoli memorizzati e scambiati tra gli utenti sulla blockchain, ed essere usati per rappresentare il possesso di opere digitali.

NGMI

Acronimo di: Not Gonna make it

Non ce la puoi fare

Livello: avanzato

Argomento: politica

Espressione usata nel contesto delle criptovalue e in particolare nelle comunità NFT, su Twitter e nei gruppi Discord relativi a NFT. Traducibile letteralmente come "non ce la puoi fare", significa che non avrai successo a causa di una decisione sbagliata o di un giudizio inadeguato. Ad esempio, se qualcuno vende un NFT in perdita mentre altri credono nel successo a lungo termine del progetto, il venditore può essere giudicato come NGMI. È l'opposto di WAGMI.

Nixon Shock

Livello: intermedio

Argomento: politica

Il Nixon Shock è un evento storico quando il 15 agosto 1971 il presidente degli Stati Uniti Richard Nixon in risposta all'aumento dell'inflazione annunciò la fine del convertibilità del dollaro in oro.

Questa decisione ha avuto un impatto profondo sull'economia globale e ha segnato l'inizio del sistema monetario basato sulla fiducia, in cui il valore delle valute è determinato principalmente dalla loro domanda e dalla loro offerta sul mercato.

Sebbene le azioni di Nixon non abolivano formalmente l'esistente sistema di scambio finanziario internazionale di Bretton Woods, la sospensione di una delle sue componenti chiave rese di fatto inoperante il sistema di Bretton Woods. Sebbene Nixon avesse pubblicamente dichiarato la sua intenzione di riprendere la convertibilità diretta del dollaro dopo l'attuazione delle riforme del sistema di Bretton Woods, tutti i tentativi di riforma si rivelarono infruttuosi. Dal 1973

il regime basato sulla libera fluttuazione delle valute fiat ha di fatto sostituito il sistema di Bretton Woods per le altre valute globali.

nLockTime

Livello: avanzato

Argomento: tecnologia

nLockTime è un parametro di una transazione che se impostato impone un tempo minimo prima del quale la transazione non può essere accettata in un blocco.

Nella versione iniziale di Bitcoin, i nodi non trasmettevano né minavano transazioni con nLockTime uguale o superiore all'altezza del blocco corrente (a meno che tutti i numeri di sequenza degli input fossero 0xffffffff), tuttavia accettavano blocchi contenenti transazioni con qualsiasi valore di nLockTime. In Bitcoin 0.1.6, l'interpretazione di nLockTime è stata regolata per consentire anche lock time-based. Poi, a partire dal blocco 31001 (dicembre 2009), le restrizioni nLockTime sono state attivate come una regola che si applicava anche all'accettazione dei blocchi. Poiché il timestamp inserito nel blocco dal miner non è preciso, a luglio 2016 i lock time-based sono stati modificati come stabilito dal BIP 113 per operare sul Median time-past invece del timestamp del blocco.

Anche se ogni transazione contiene il campo nLockTime, ogni wallet fino a poco tempo fa impostava nLockTime a 0, il che significa che la transazione era valida in qualsiasi blocco. A partire da Bitcoin Core 0.11.0, ogni transazione normale generata automaticamente ha iniziato a includere un nLockTime impostato su un'altezza di blocco recente come un modo per rendere meno redditizio l'ipotetico Fee sniping.

All'inizio del 2019 circa il 20% di tutte le transazioni bitcoin impostano un valore nLockTime diverso da zero.

nLockTime è un parametro di una transazione, che, se qualsiasi input lo indica (avendo nSequence non uguale a UINT_MAX), impone un tempo minimo (specificato sia in tempo unix che in altezza di blocco), prima del quale la transazione non può essere accettata in un blocco. Se tutti gli ingressi in una transazione hanno nSequence uguale a UINT_MAX (0xFFFFFFFF), allora nLockTime viene ignorato.

Se nLockTime < 500000000 Specifica il numero di blocco dopo il quale questa transazione può essere inclusa in un blocco. Altrimenti specifica il timestamp UNIX dopo il quale questa transazione può essere inclusa in un blocco. Dall'adozione del BIP 113, nLockTime basato sul tempo viene confrontato con il Median time-past, il tempo passato mediano degli 11 blocchi (il timestamp mediano degli 11 blocchi che precedono il blocco in cui la transazione viene estratta), e non il tempo del blocco stesso. Il tempo mediano passato tende a

ritardare il tempo unix corrente di circa un'ora (più o meno), ma a differenza del tempo del blocco aumenta monotonicamente.

Per il relay della transazione, nLockTime deve essere minore o uguale al block height corrente (block-based) o minore o uguale al tempo mediano passato corrente (if time based). Questo assicura che la transazione possa essere inclusa nel blocco successivo.

Il comportamento di nLockTime di una transazione può essere modificato dal numero di sequenza di un ingresso quando si usa OP_CHECKSEQUENCEVERIFY. Questo particolare opcode è usato all'interno degli script di input per asserire che il numero di sequenza dell'input, che nelle transazioni normali è impostato a UINT_MAX, è maggiore o uguale all'elemento superiore dello stack (di solito il nLockTime della transazione). OP_CHECKSEQUENCEVERIFY è usato in alcuni protocolli Layer 2.

No-Coiner

Livello: intermedio

Argomento: politica

Un nocoiner è una persona che non possiede Bitcoin o altre criptovalute. Le ragioni dietro questa scelta possono essere molteplici e variegate, consapevoli o meno. In alcuni casi, il termine viene utilizzato per indicare le persone che deliberatamente scelgono di non possedere criptovalute. Alcuni ritengono che Bitcoin non sia affidabile, anonimo o sicuro, o che abbia poco o nessun valore. Altri possono sospettare che sia uno schema Ponzi destinato a fallire.

L'etichetta nocoiner deriva dall'atteggiamento o dalla filosofia nei confronti delle criptovalute; in altre parole, non si tratta solo di scetticismo, ma di una convinzione ferma che le valute digitali non abbiano un posto nel mondo. Nonostante le evidenze dei casi d'uso delle criptovalute, i nocoiner tendono a vedere solo il loro utilizzo da parte di criminali e altre attività illecite.

Il termine nocoiner viene anche utilizzato per indicare coloro che criticano Bitcoin senza comprenderne appieno il funzionamento o l'importanza, come la decentralizzazione.

La maggior parte dei nocoiner ha in comune la mancanza di comprensione dell'importanza della decentralizzazione.

Node

Nodo

Livello: base

Argomento: tecnologia

Un nodo è un computer che interagisce con altri nodi per formare la rete.

Nel caso di una rete p2p, quale è anche la rete bitcoin, i nodi non sono organizzati gerarchicamente ma sono tra loro pari, tutti i nodi condividono l'onere di fornire servizi di rete, aiutandola a mantenere la sua forma decentralizzata.

I nodi bitcoin convalidano, trasmettono e richiedono nuovi blocchi e la mempool a e dai peer della rete. Se i nodi eseguono un software compatibile, si ottiene il consenso.

Il numero di nodi è fondamentale per proteggere la rete da modifiche del codice sorgente, riorganizzazioni e altri cambiamenti di protocollo dannosi o casuali.

I nodi bitcoin possono essere classificati secondo diverse tipologie in funzione dei servizi che gestiscono:

- Full node, che mantiene e tiene aggiornata una copia della blockchain
- SPV o Lightweight wallet, è un nodo che gestisce un wallet ma non mantiene copia della blockchain e non contribuiscono alla sicurezza della rete, si limitano a raccogliere le informazioni dai full node
- Nodo di mining, esegue le funzioni di mining, in modalità "solo" o collegandosi a mining pool

Non custodial

Livello: base

Argomento: legale

Un non-custodial wallet, o self custodial, è un tipo di wallet le cui chiavi private sono conosciute e controllate direttamente dall'utente, gli utenti sono gli unici custodi delle loro chiavi private e, quindi, degli asset che vi vengono conservati. Questo significa che l'utente ha il pieno controllo dei fondi e fintanto che le chiavi private sono conosciute solo all'utente, i suoi fondi non possono essere bloccati o gestiti da terze parti.

I non-custodial wallet, poiché eliminano la necessità di una terza parte fidata, per certi aspetti sono più sicuri dei custodial wallet.

Esistono diversi tipi di non-custodial wallet, tra cui quelli basati su browser, i wallet software per telefoni cellulari e computer e gli hardware wallet. I wallet hardware, disponibili in vari formati, si dice che offrano il massimo livello di sicurezza per la conservazione delle criptovalute. Questi wallet assomigliano a unità USB ma sono dotati di un display e di pulsanti fisici.

I non-custodial wallet sono semplici da configurare. Per i wallet software non-custodial, gli utenti devono scaricare il software, salvare in un posto sicuro frase mnemonica o Seed Recovery Phrase, ovvero una chiave composta da una stringa di 12, 18 o 24 parole corrispondenti alla chiave privata, e impostare una password.

Inoltre, se gli utenti dimenticano la password, la frase mnemonica serve come backup per poter ripristinare la chiave privata e avere il controllo dei propri

fondi.

Questo comporta però c'è poco da fare per gli utenti dei wallet nel caso in cui perdano le chiavi o non adottino le misure di sicurezza operative necessarie per proteggere la password e le chiavi. Se un utente perde, cancella o dimentica la propria chiave, rischia di perdere completamente l'accesso ai propri fondi.

Pertanto, per proteggere adeguatamente queste informazioni, gli utenti di non-custodial wallet sono tenuti ad adottare misure supplementari per garantire la sicurezza della password e del wallet.

I non-custodial wallet in alcuni contesti vengono chiamati un-hosted Wallet, termine ad esempio utilizzato dal MiCA, il regolamento Europeo sui mercati nelle criptovalute.

Non-deterministic wallets

Wallet non deterministici

Livello: intermedio

Argomento: tecnologia

I wallet non deterministici generano tutte le coppie di chiavi private/pubbliche in modo casuale indipendenti l'una dall'altra.

Sono anche chiamati Wallet JBOK, Just-a-Bunch-of-Keys (Solo un gruppo di chiavi).

Nell'ottobre 2010 è stato aggiunto un keypool buffer al wallet Bitcoin-Qt / Bitcoin Core, che ha consentito al wallet di creare una lista di indirizzi inutilizzati, invece di generare nuovi indirizzi uno per uno al momento dell'uso. Sebbene questa funzionalità consentisse backup meno frequenti rispetto a prima, il non determinismo comportava comunque il rischio di perdita della chiave se il pool si esauriva e veniva generata una nuova chiave oltre a quella salvata nel backup, costringendo quindi a fare un back-up ogni volta che venivano generate nuove chiavi.

Nonce

Livello: avanzato

Argomento: tecnologia

Il termine nonce è l'abbreviazione di number only used once, "numero usato solo una volta".
I nonce vengono spesso utilizzati sui protocolli di autenticazione e sulle funzioni di hash crittografiche.

Il nonce nelle funzioni Bitcoin viene usato nelle transazioni e nel mining

Nonce nella firma delle transazioni

Nella firma delle transazioni Bitcoin, viene utilizzato un nonce come parte integrante del processo di firma ECDSA. Il nonce di firma viene utilizzato per introdurre casualità nella firma di ogni transazione, rendendo praticamente impossibile prevedere la chiave di firma privata utilizzata per creare la firma.

Quando un utente desidera firmare una transazione Bitcoin, il nonce di firma viene generato in modo casuale. Questo nonce viene combinato con la chiave privata del mittente e l'hash del messaggio (che include i dettagli della transazione) per calcolare la firma digitale utilizzando l'algoritmo ECDSA.

L'uso di un nonce casuale è fondamentale per garantire la sicurezza della firma delle transazioni.

È ben noto nella comunità crittografica che lo schema di firma ECDSA è fragile rispetto alle vulnerabilità nella generazione dei nonce. Un attaccante può recuperare la chiave privata ECDSA di un firmatario se conosce il nonce utilizzato per generare una singola firma; se un firmatario firma due messaggi distinti con lo stesso nonce; se un firmatario firma più messaggi con nonce inaspettatamente brevi; se l'attaccante può apprendere i bit più significativi di molti nonce di firma, e così via.
Quando la chiave privata può essere facilmente determinata la sicurezza dei fondi gestiti con quella chiave privata viene compromessa.

Una volta generato il nonce di firma, viene utilizzato insieme alla chiave privata per calcolare la firma digitale, che viene poi inclusa nella transazione Bitcoin come parte dell'input di firma scriptSig.
La firma consente al destinatario della transazione di verificare che la transazione sia stata autorizzata dal proprietario della chiave privata corrispondente.

In sintesi, il nonce di firma viene utilizzato per garantire l'imprevedibilità della firma ECDSA di ogni transazione Bitcoin, aggiungendo casualità al processo di firma e proteggendo così la sicurezza del sistema.

Nonce nel mining

Nel contesto del mining, il nonce è il numero che i miner devono trovare per minare un blocco. Questo numero, quando aggiunto all'hash di un blocco, deve soddisfare le condizioni del livello di difficoltà prestabilito.

Quando un miner trova un nonce che soddisfa i criteri richiesti, può creare il blocco e aggiungerlo alla blockchain, ricevendo come ricompensa la nuova criptovaluta.

I miner devono tentare di trovare un nonce valido eseguendo numerosi calcoli per ottenere un hash di blocco che soddisfi determinati requisiti, ovvero un certo numero di zeri iniziali: maggiori sono gli zeri richiesti e maggiore è la difficoltà. Durante la competizione per estrarre un nuovo blocco, il primo miner che trova

un nonce che produce un hash di blocco valido ha il diritto di aggiungere il blocco successivo alla blockchain e viene ricompensato per questo.

In altre parole, il processo di mining coinvolge i miner che eseguono numerose funzioni di hash con diversi valori di nonce fino a quando non viene prodotto un output valido. Se l'output hash di un miner soddisfa una soglia predeterminata, il blocco viene considerato valido e viene aggiunto alla blockchain. Se l'output non è valido, il miner continua a provare con diversi valori di nonce. Una volta che un nuovo blocco viene estratto e convalidato con successo, il processo ricomincia.

Nel contesto di Bitcoin e della maggior parte dei sistemi Proof of Work, il nonce è semplicemente un numero casuale utilizzato dai miner per iterare l'output dei calcoli di hash. I miner adottano un approccio di tentativi ed errori, provando diversi valori di nonce, poiché la probabilità di indovinare con precisione un nonce valido è estremamente bassa.

Nostr

Livello: base

Argomento: tecnologia

Nostr è un protocollo di rete decentralizzato per un sistema di social networking distribuito.
Il nome è un acronimo di Notes and Other Stuff Transmitted by Relay, Note e Altre Cose Trasmesse da Relè.
I post sono resistenti alla censura e sono validati in modo crittografico.

Nostr è un progetto open source che mira a creare una piattaforma di social media decentralizzata e resistente alla censura. Il protocollo Nostr è progettato per essere semplice e facile da usare, consentendo a chiunque di creare e partecipare a una rete sociale senza bisogno di un'autorità centrale.

I post su Nostr sono resistenti alla censura perché sono distribuiti su una rete di chiamati Relay. Ciò significa che se un nodo tenta di censurare un post, gli altri nodi continueranno a distribuirlo. I post sono anche validati in modo crittografico, il che significa che è impossibile falsificarli.

Nostr è ancora in fase di sviluppo, ma ha il potenziale di rivoluzionare il modo in cui interagiamo con i social media. Offrendo un'alternativa alle piattaforme centralizzate, Nostr può aiutare a proteggere la libertà di espressione e la privacy degli utenti.

La sua adozione ha registrato una marcata crescita tra i Bitcoiner, grazie alla sua affinità con alcuni concetti cari ai bitcoiner:

- decentralizzazione e resistenza alla censura;

- gli account su Nostr possono essere creati dagli utenti seguendo lo stesso principio con cui vengono creati gli indirizzi Bitcoin, essenzialmente costituendo coppie di chiavi pubbliche/private;
- su Nostr sono state implementate estensioni che permettono il trasferimento di pagamenti in Bitcoin tramite la Lightning Network, chiamati zap, consentendo quindi anche transazioni di importi minimi a costi e tempi di trasferimento estremamente ridotti.

Poiché si tratta di un protocollo aperto, non esiste un unico client, ma sono stati sviluppati vari client adattabili a diversi contesti, oltre a numerose applicazioni.

NYK, NYC

Acronimo di: Not Your Keys, Not Your Coins

Livello: base

Argomento: politica

Not Your Keys, Not Your Coins, in italiano se le chiavi non sono tue neanche le criptovalute, è un detto che significa che se non si controllano le proprie chiavi private, allora non si controllano veramente le proprie criptovalute.

È un'espressione usata per enfatizzare l'importanza per la gestione delle proprie criptovalute del controllo personale delle chiavi private.

Questo è importante perché le chiavi private sono ciò che permette di accedere ai propri fondi e, se qualcuno altro le possiede può in pratica controllare le criptovalute, spendendole o trasferendo i fondi ad un altro indirizzo.
Pertanto, è importante mantenere il controllo delle proprie chiavi private per garantire che nessun altro possa accedere ai propri fondi, o decidere cosa si possa o non si possa fare con i propri conti.

I wallet che rientrano nella categoria "Not Your Keys" sono quelli definiti come custodial o Hosted wallet.

Quando si detengono le proprie criptovalute su un exchange centralizzato o su un altro servizio di custodia, si sta essenzialmente dando le chiavi private a qualcun altro. Questo significa che quell'entità ha il controllo dei fondi e può di fatto decidere cosa farne.

OAM

Organismo per la gestione degli Elenchi degli Agenti in attività finanziaria e dei Mediatori creditizi

Livello: intermedio

Argomento: legale

L'OAM è l'Organismo per le attività creditizie e finanziarie, un'autorità amministrativa indipendente istituita ai sensi del Decreto Legislativo 267/2000. È preposto alla vigilanza sulle attività svolte da soggetti che operano nel settore finanziario, quali agenti in attività finanziaria, mediatori creditizi, istituti di pagamento e di moneta elettronica, operatori finanziari e società di gestione del risparmio

Nel 2022, l'OAM ha assunto la competenza in materia di contrasto al riciclaggio e al finanziamento del terrorismo, in particolare per quanto riguarda i prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale (VASP), tra i quali anche gli exchange di criptovalute.
A tal fine, l'OAM ha istituito un registro dedicato ai VASP, che sono obbligati ad iscriversi e a trasmettere periodicamente all'OAM i dati dei clienti e le informazioni sulle operazioni effettuate.

I VASP sono soggetti a una serie di obblighi di trasparenza e di prevenzione del riciclaggio e del finanziamento del terrorismo. In particolare, devono:

- KYC: Istituire una procedura di adeguata verifica della clientela, al fine di identificare i clienti e acquisire informazioni sulle loro attività economiche e finanziarie;
- Monitorare le operazioni effettuate dai clienti, al fine di rilevare eventuali operazioni sospette;
- Sospendere le operazioni sospette e segnalarle all'UIF, l'Unità di informazione finanziaria per l'Italia.

L'iscrizione al registro dell'OAM è obbligatoria per i VASP che operano sul territorio italiano. La mancata iscrizione è punita con sanzioni amministrative pecuniarie.

I VASP devono quindi continuamente raccogliere e trasmettere i dati dei loro clienti e le informazioni sulle operazioni finanziarie da loro effettuate.

Con l'entrata in vigore del Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività (MiCAR) e del relativo decreto di adeguamento italiano (D.Lgs. n. 129 del 5 settembre 2024), l'obbligo di trasmissione dei dati all'OAM da parte dei VASP (Virtual Asset Service Providers) cessa a partire dal secondo trimestre del 2025.

Questo significa che l'ultimo invio di dati da parte dei VASP all'OAM riguarderà le informazioni relative al primo trimestre del 2025.

La Circolare OAM n. 55/24 del 6 dicembre 2024 ha chiarito questo aspetto, indicando che l'obbligo di trasmissione dei flussi di dati cesserà con l'invio delle informazioni relative al primo trimestre dell'anno 2025.

OFAC

Acronimo di: Office of Foreign Assets Control

Ufficio per il controllo dei beni esteri del Dipartimento del Tesoro statunitense

Livello: intermedio

Argomento: legale

L'OFAC, Office of Foreign Assets Control (Ufficio per il controllo dei beni esteri) è un'agenzia di intelligence finanziaria e di applicazione del Dipartimento del Tesoro degli Stati Uniti.

L'OFAC amministra e applica sanzioni economiche e commerciali a sostegno degli obiettivi di politica estera e di sicurezza nazionale degli Stati Uniti. In base ai poteri presidenziali di emergenza nazionale, l'OFAC svolge le sue attività contro Stati stranieri e una serie di altre organizzazioni e individui, come i gruppi terroristici, ritenuti dagli Stati Uniti una minaccia per la loro sicurezza nazionale.

Nel settore delle criptovalute ha preso diverse iniziative controverse, sanzionando servizi come Blender colpevole di aver facilitato attività di riciclaggio di criptovalute in favore del Lazarus Group, un gruppo di cyber-criminali vicino al DPRK, il governo della Corea del Nord.

Ma soprattutto nell'agosto 2022, ha emesso un atto con cui ha incluso il sito del software Tornado Cash e 45 specifici indirizzi ospitati sulla rete Ethereum nella lista delle Specially Designated Nationals and Blocked Persons, entità ed individui stranieri con i quali è vietato ai cittadini americani di interagire, a pena di sanzioni amministrative e pecuniarie durissime.

Nei giorni successivi il ventinovenne ingegnere Alexey Pertsev, ingegnere informatico russo e maggiore contributore del codice di Tornado Cash, è stato arrestato nei Paesi Bassi con una non meglio circostanziata accusa di favoreggiamento di reati finanziari e di riciclaggio. Le autorità olandesi non hanno saputo specificare nel dettaglio le contestazioni, ma il giudice dell'udienza preliminare ha confermato l'arresto e fissato la prossima udienza tra 90 giorni.

Il Governo statunitense ha poi abbattuto i server che ospitavano la landing page del servizio di mixing ed imposto a Github.com, la più nota piattaforma che ospita il codice di centinaia di migliaia di programmi informatici open-source, di cancellare il repository di Tornado Cash. Ancora, decine di provider di servizi connessi all'utilizzo di valute virtuali, tra i quali i maggiori exchange, le applicazioni decentralizzate di DeFi come Aave e Compound, l'emittente di stablecoin USDC hanno bloccato le transazioni in ingresso ed in uscita a tutti quegli utenti che erano entrati in contatto con gli indirizzi incriminati.

Off Chain

Livello: base

Argomento: tecnologia

Le transazioni Bitcoin che non vengono registrate nella block chain sono definite off-chain.

Le transazioni on-chain sono quelle che vengono registrate sulla blockchain.

Le transazioni di Lightning Network sono un esempio di transazioni off-chain. Queste transazioni avvengono off chain fino a quando i saldi finali non vengono regolati on-chain, riducendo così i tempi e le commissioni di transazione.

Una transazione off-chain non richiede i servizi dei miner non richiede i servizi dei miner necessari per aggiungerla ad un blocco della blockchain.

Le transazioni off-chain sono generalmente più veloci delle transazioni on-chain, possono comportare commissioni più basse, essere effettuate istantaneamente e offrire maggiore anonimato.

Le transazioni on-chain si riflettono sul ledger distribuito.
La verifica del ledger viene effettuata dai miner per convalidare la transazione. Poiché tutto avviene sulla chain, i dettagli della transazione vengono registrati. La transazione viene aggiunta al ledger distribuito e resa visibile sull'intera rete. Questo la rende irreversibile.

Se si considerano le altre transazioni in coda nella mempool e i numerosi passaggi da compiere, è facile capire perché le transazioni on-chain richiedano più tempo per andare a buon fine. Inoltre, le transazioni on-chain comportano costi potenzialmente elevati. Questi sono i motivi per cui per certi casi d'uso gli utenti possano preferire le transazioni off chain.

Le transazioni off-chain, invece, avvengono quasi istantaneamente attraverso alcuni metodi diversi. Senza dover attendere le conferme della rete blockchain, le transazioni sono più veloci. Le transazioni on-chain richiedono la convalida da parte di validatori e finiscono per comportare costi elevati. Mentre le transazioni off-chain sono solitamente a basso costo. Queste transazioni non sono visibili sulla blockchain e offrono maggiore privacy. Le transazioni off-chain possono avvenire tra due parti attraverso un accordo di trasferimento. Una terza parte potrebbe fungere da garante per garantire il successo della transazione. Oggi anche alcuni processori di pagamento operano in questo senso.

Le transazioni off chain che avvengono al di fuori di una rete blockchain possono essere effettuate in diversi modi.
Uno dei metodi consiste nell'utilizzare una rete di pagamento come Lightning Network.
Un altro metodo comune di transazione off chain è quello di scambiare le chiavi private di un portafoglio esistente. Con questo metodo, un nuovo proprietario viene assegnato a un portafoglio specifico. Questo metodo non altera la rete blockchain ed è un modo istantaneo per eseguire la transazione. Alcuni exchange decentralizzati o DEX hanno adottato il ruolo di escrow per fungere da garante tra due soggetti disposti a effettuare una transazione off chain.

Official currency

Livello: avanzato

Argomento: politica

La traduzione letterale in italiano di Official currency può essere Valuta ufficiale.

Il termine currency, traducibile con Valuta, con l'arrivo dei Bitcoin si è arrichito di nuovi significati. Sono nate le cryptocurrency o criptovalute, delle quali la prima è più importante è appunto Bitcoin.

Il regolamento Europeo sui mercati nelle criptovalute, il MiCA, nel regolare il settore si trova nella necessità di dover differenziare tra valute cripto e le altre valute più tradizionali.

Nel settore delle critpovalute esiste già un termine allo scopo: valute Fiat, o valute a corso forzoso. Ma evidentemente questo termine (che non viene mai usato nel MiCA) non è gradito, e quindi nel regolamento viene utilizzato il termine *Official currency*, definito in questo modo:

"*Per Official currency si intende la valuta ufficiale di un paese emessa da una banca centrale o da un'altra autorità monetaria.*"

Da notare come per definirle, venga fatto riferimento a chi emette queste valute, e solo non ai paesi che adottano la valuta in modo ufficiale, perché dal 2021 esiste l'importante precedente dello stato di El Salvador che ha dichiarato Bitcoin moneta a corso legale.

Gli stati o gruppi di stati adottano quindi una valuta ufficiale, per lo più attraverso la propria banca centrale in regime di monopolio.

Parlare però di "propria banca centrale" può essere una pessima approssimazione, il rapporto tra gli stati e questi soggetti emittenti è variegato: ci sono stati che hanno una propria valuta, unioni monetarie come l'Euro o come le comunità finanziaria africane, stati che utilizzano la propria valuta e la valuta di un altro paese, stati che non hanno la loro moneta e utilizzano la valuta di un altro paese.

Inoltre la maggior parte delle banche centrali sono state privatizzate, e in alcuni stati esistono più istituti di emissione, e alcuni stati hanno una valuta ufficiale che viene gestita.

La banca centrale può essere più o meno indipendente dal potere politico. Il modello più noto di banca centrale indipendente è quello della Bundesbank tedesca, nel quale il potere politico non ha il potere di ratificare o invalidare le decisioni prese dalla banca. La Bundesbank è stata presa a modello da tutte le banche centrali dei Paesi che sono entrati nella zona euro. Il modello alternativo è quello Reserve Bank of New Zealand, nel quale gli obiettivi sono fissati dal governo. Nel pensiero economico contemporaneo l'indipendenza della banca centrale è generalmente considerata una caratteristica vantaggiosa per

l'economia, anche se esiste un certo numero di studiosi critici di questo principio. Vi possono essere banche centrali completamente di proprietà dello Stato (Nuova Zelanda e Norvegia) e altre aventi partecipazioni parzialmente o totalmente private (Banca d'Italia). La Federal Reserve statunitense è una banca centrale di proprietà di privati.

On Chain

Livello: intermedio

Argomento: tecnologia

Registrato sulla blockchain e trasmesso a tutti i nodi della rete.

On-chain è un termine utilizzato per descrivere qualsiasi dato registrato sulla blockchain di Bitcoin, in contrasto con le transazioni o i dati off-chain, che non sono memorizzati sulla blockchain. I dati on-chain sono sempre transazioni Bitcoin, mentre i dati off-chain possono essere transazioni Bitcoin non confermate o qualsiasi altro tipo di dati.

Un sistema blockchain è essenzialmente una rete che contiene un ledger o libro mastro distribuito che può essere considerato come un database condiviso. Le transazioni che vengono registrate sulla blockchain stessa e condivise con tutti i partecipanti sono effettuate on-chain.

Ogni volta che viene effettuata una nuova transazione, è necessario aggiungerla ad un nuovo blocco nella blockchain perché possa essere considerata confermata, ed esistono protocolli di consenso che devono essere seguiti affinché la transazione sia considerata valida.

Le transazioni on-chain sono quelle che avvengono su una blockchain e che si riflettono sulla distribuzione e sul libro mastro pubblico. Le transazioni on-chain sono quelle che sono già state convalidate e autenticate dai miner o dai validatori. Queste possono a loro volta portare a un aggiornamento generale della rete blockchain stessa.

Lightning Network è un interessante esempio di protocollo che consente di gestire le transazioni off-chain, considerato una soluzione di livello 2, un second layer, che si trova sopra Bitcoin, consentendo transazioni off-chain più rapide e potenzialmente più economiche rispetto alle transazioni on-chain, garantite comunque dalla sicurezza delle transazioni on-chain.

Affinché una transazione on-chain sia completa, è necessario che vi sia un numero concordato di conferme, mentre il tempo necessario per il completamento di una transazione on-chain dipende anche dalla congestione della rete. A volte le transazioni vengono ritardate se c'è un grande volume di transazioni che devono essere confermate.

Se confrontiamo questo aspetto con le transazioni off-chain, questa è la seconda variante quando si parla di variazione delle transazioni. Le differenze sono

molteplici: gli accordi per le transazioni off-chain avvengono in realtà al di fuori della blockchain e il protocollo utilizzato per le transazioni off-chain può essere analogo a quello utilizzato nelle piattaforme di pagamento.

Ciò significa che le parti coinvolte nella transazione hanno la possibilità di scegliere un accordo al di fuori della blockchain, e il passo successivo può potenzialmente coinvolgere una terza parte il cui ruolo è quello di confermare il completamento della transazione e di certificare che l'accordo è stato rispettato da entrambe le parti.

onion routing

Livello: avanzato

Argomento: tecnologia

L'onion routing è una tecnologia di privacy e sicurezza online che permette agli utenti di navigare in modo anonimo su internet.
In sostanza, l'onion routing protegge la privacy dell'utente crittando il traffico di rete e nascondendo l'indirizzo IP dell'utente.

Il termine onion può essere tradotto "a cipolla", il nome onion routing deriva dalla sua architettura a layer o strati, analoghi agli strati di una cipolla.
Quando un utente invia una richiesta su una rete onion, la richiesta viene criptata e inviata attraverso una serie di nodi intermediari chiamati "onion routers". Ogni nodo rimuove un layer di crittografia per accedere all'indirizzo del nodo successivo, fino a quando la richiesta arriva alla destinazione finale.

Poiché ogni nodo intermedio conosce solo l'indirizzo del nodo precedente e successivo, diventa molto difficile per un osservatore esterno monitorare la posizione dell'utente o tracciare le sue attività. Questo rende l'onion routing particolarmente utile per navigare in modo anonimo su Internet o per proteggere la privacy in situazioni in cui la sorveglianza online è un problema.

Quando l'ultimo strato viene decifrato, il messaggio arriva a destinazione. Il mittente rimane anonimo perché ogni intermediario conosce solo la posizione dei nodi immediatamente precedenti e successivi.

Anche se è stata originariamente sviluppata per la navigazione anonima sul web, l'onion routing è stata adottata anche in altre applicazioni che richiedono privacy e anonimato, inclusa la rete Bitcoin.

In Bitcoin, l'onion routing è utilizzato per migliorare la privacy delle transazioni tra gli utenti. In particolare, il protocollo di onion routing viene utilizzato per nascondere l'indirizzo IP dell'utente che invia una transazione e l'indirizzo IP del destinatario della transazione.

Anche Lightning Network è progettata per garantire un elevato livello di anonimato e riservatezza per i flussi di pagamento attraverso onion routing: la catena di HTLC utilizza l'onion routing, il che significa che il messaggio HTLC è avvolto

in più strati di crittografia, uno per ogni hop coinvolto nel canale di comunicazione.
Nell'implementazione più rispettosa della privacy, questo onion routing viene costruito dal pagatore, e gli hop intermedi non acquisiscono conoscenza della sorgente e della destinazione della catena HTLC.

L'onion routing rende difficile tracciare le transazioni di Bitcoin fino ai loro utenti effettivi, migliorando notevolmente la privacy e l'anonimato delle transazioni. Tuttavia, è importante notare che l'onion routing non è una soluzione perfetta per la privacy e che altri fattori, come l'uso di indirizzi di Bitcoin riusabili o la rivelazione di informazioni personali in altri contesti online, possono ancora compromettere l'anonimato degli utenti di Bitcoin.

Sono state proposte tecniche aggiuntive per migliorare la privacy onion routing su Lightning Network, come la tecnica Trampoline e il Route blinding.

OP_CAT

Livello: avanzato

Argomento: tecnologia

OP_CAT è uno degli opcode del linguaggio Bitcoin Script.

Il nome fa riferimento a CAT, abbreviazione di "concatenate" (concatenare in italiano), poiché questo operatore consente di unire due elementi all'interno di uno script.

Vulnerabilità e disabilitazione Inizialmente introdotto nelle prime versioni, Satoshi Nakamoto lo ha disabilitato nel 2010 a causa di potenziali vulnerabilità sfruttabili presenti nelle implementazioni originali che minacciavano la sicurezza della rete Bitcoin.
Ad esempio, OP_CAT, se combinato con OP_DUP (duplicato) e utilizzato ripetutamente per duplicare un valore anche inizialmente di 1 solo byte nello stack, poteva causare un'eccessiva utilizzazione della memoria del nodo, consentendo un potenziale attacco Denial of Service.

Dato che OP_CAT è stato disabilitato, qualsiasi script che lo includa renderà la transazione non valida indipendentemente dal contesto.

Rinnovato interesse Recentemente c'è stato un rinnovato interesse per l'operatore OP_CAT e una sua possibile riabilitazione, per diversi motivi:

- Il problema relativo alla vulnerabilità è stato mitigato imponendo un limite di 520 byte sugli elementi dello stack
- la combinazione di OP_CAT con le firme di Schnorr, introdotte in Bitcoin con il softfork taproot, consentono di implementare negli script bitcoin diversi casi d'uso.

OP_CAT potrebbe aprire la strada a interessanti applicazioni basate sugli script Bitcoin, come:

- Covenant più complessi e *introspettivi*: op_checksig consente di simulare la firma di un pezzo di dati nello stack. Ciò significa che con OP_CAT e SHA256 possiamo aggiungere elementi di testo chiaro allo stack, unirli in un hash e confrontarli con una firma predefinita che contiene un covenant. Ad esempio, la firma e il risultato dell'hash corrispondono solo se la transazione costruita rispetta le restrizioni di spesa. Questo permette di aggiungere molte funzionalità espressive alle transazioni Bitcoin.
- Verifica delle Merkle proof (prove di Merkle). Poiché le Merkle proof richiedono la concatenazione dell'hash di due nodi foglia, che vengono quindi nuovamente hashati, per verificare una prova di Merkle data un percorso di Merkle, dobbiamo avere OP_CAT. Con la verifica delle Merkle proof possiamo creare cose come ponti di client leggeri senza fiducia da e verso Bitcoin, migliorando la sicurezza L2 per sidechain multisig esistenti e opzioni custodial.
- Vault (Casseforti). OP_CAT facilita la creazione di covenant ricorsivi attraverso meccanismi come lo switch di valore e il preimage della transazione, utili per implementare funzionalità di tipo vault.

Un argomento contro OP_CAT è che da solo non è sufficiente per realizzare appieno molte delle funzioni di calcolo generico che si potrebbero desiderare da Bitcoin.

Alcuni altri op_codes che sono stati discussi sono op_ctv (che confronta gli output di una transazione con un hash dato e richiede che siano uguali), op_csfs (che consente la verifica di qualsiasi firma su qualsiasi messaggio).
La presenza di questi op_codes potrebbe notevolmente agevolare lo sviluppo e la complessità dei covenant e delle applicazioni costruibili su Bitcoin; tuttavia, sono significativamente più complessi e devono affrontare metodologie di approvazione politica più rigorose rispetto a OP_CAT.

OP_RETURN

Livello: avanzato

Argomento: tecnologia

OP_RETURN è un opcode nel sistema di scripting di bitcoin che consente l'inclusione di una piccola quantità di dati arbitrari in una transazione.
Questo codice operativo contrassegna immediatamente l'output della transazione come non spendibile, garantendo che l'output non possa essere utilizzato come input in una transazione successiva.

In programmazione, l'operatore `return` è un'istruzione che termina l'esecuzione di una funzione e restituisce il controllo alla funzione chiamante. Può anche restituire un valore alla funzione chiamante.

Nel caso di Bitcoin, questa caratteristica viene utilizzata principalmente per incorporare dati arbitrari nella blockchain.

Qualsiasi output di transazione con questo opcode non è spendibile, ma i dati dopo OP_RETURN rimangono permanentemente sulla blockchain. Questo è diventato un modo per dichiarare che l'output non può essere speso ed è qui solo per i dati.

Gli output script che iniziano con OP_RETURN, chiamati data carrier output, possono avere un importo pari a zero. L'opcode OP_RETURN fa sì che lo script fallisca immediatamente, indipendentemente da ciò che segue, quindi questi output non possono mai essere spesi. Ciò significa che i full node non hanno bisogno di tenerne traccia, una caratteristica di Bitcoin Core che consente agli utenti di memorizzare piccole quantità di dati arbitrari nella blockchain senza aumentare le dimensioni dell'UTXO set. Poiché gli output non sono spendibili, non sono anti-economici: qualsiasi satoshi assegnato a essi diventa permanentemente non spendibile, quindi consentire che l'importo sia zero garantisce che i satoshi non vengano distrutti.

Su Bitcoin Core, il parametro datacarriersize imposta la dimensione massima del datacarrier, ovvero dei dati che possono essere inseriti con OP_RETURN, o meglio la lunghezza totale dello script, argomento al centro di diversi dibattiti all'interno della comunità.

Opcode

Livello: avanzato

Argomento: tecnologia

Un opcode, o codice operativo, è un comando di base di alcuni linguaggi di computer.

Il linguaggio di scripting di Bitcoin, chiamato Script, ha un suo insieme di opcode.

Bitcoin Script ha circa 100 opcode.

Gli opcode eseguono funzioni all'interno di uno ScriptPubKey o di un ScriptSig.

Ciascun opcode è rappresentato da codice simbolico e ha un suo valore numerico, esegue una funzione limitata e predefinita.

La combinazione di questi opcode con i dati aggiuntivi come indirizzi, chiavi pubbliche e firme può produrre script Bitcoin che consentono di fare operazioni più o meno complesse.

Ad esempio, uno degli script Bitcoin più comuni è P2PKH, che è composto da 4 opcode e un hash di chiave pubblica. Questo script è un tipo di ScriptPubKey o locking script, che viene utilizzato per bloccare bitcoin in modo tale che

solo qualcuno in grado di produrre la chiave pubblica e una firma valida possa spenderlo.

Tramite questi opcode non è possibile moltiplicare, dividere o combinare oggetti sullo stack.

Nelle versioni iniziali, Satoshi Nakamoto aveva incluso un numero maggiore di opcode nel linguaggio script, ma ne ha disabilitato alcuni per vari motivi tecnici o di sicurezza nel 2010, tra cui OP_OR, OP_MUL (moltiplica), OP_DIV (dividi) e OP_CAT (concatena).
I codici operativi disabilitati sono stati rimossi perché le loro implementazioni originali presentavano vulnerabilità sfruttabili che potevano compromettere la sicurezza della rete Bitcoin.

Ci sono alcune proposte per estendere gli opcode, o ripristinare alcuni di quelli disabilitati, ad esempio OP_CAT.

open interest

Livello: intermedio

Argomento: finanza

L'open interest, in italiano interesse aperto, rappresenta il numero di contratti futures o opzioni su un determinato sottostante che sono aperti in un dato momento, e che non sono ancora stati chiusi o liquidati. In altre parole, è la misura della somma di tutte le posizioni lunghe e corte aperte su un determinato strumento finanziario derivato.

Differenza tra Open Interest e Volume È importante non confondere l'open interest con il volume. Il volume rappresenta il numero di contratti che sono stati scambiati durante un determinato periodo di tempo, mentre l'open interest indica il numero di contratti che sono ancora aperti in un dato momento.

Come si calcola l'Open Interest L'open interest viene calcolato sommando il numero di contratti acquistati (posizioni lunghe) che non sono ancora stati venduti e il numero di contratti venduti (posizioni corte) che non sono ancora stati riacquistati.

A cosa serve l'Open Interest L'open interest è un indicatore importante per i trader perché può fornire informazioni sulla forza e sul direzione di un trend, sulla liquidità e sull'attività di trading per uno strumento finanziario specifico.
Un aumento dell'open interest può indicare che nuovi partecipanti stanno entrando nel mercato o che gli attuali partecipanti stanno ampliando le loro posizioni. Al contrario, una diminuzione dell'open interest potrebbe indicare che i trader stanno chiudendo le loro posizioni o riducendo la loro attività nel mercato.

In generale, un aumento dell'open interest durante un trend rialzista è considerato un segnale di forza del trend, mentre un calo dell'open interest durante un trend rialzista può essere un segnale di indebolimento del trend e di una possibile inversione.

Come utilizzare l'Open Interest nel trading L'open interest può essere utilizzato in combinazione con altri indicatori tecnici per individuare potenziali opportunità di trading. Ad esempio, un trader potrebbe cercare di acquistare un futures o un'opzione con un open interest in aumento se ritiene che il trend stia per rafforzarsi. Al contrario, un trader potrebbe cercare di vendere un futures o un'opzione con un open interest in calo se ritiene che il trend stia per invertirsi.

È importante sottolineare che l'open interest è solo uno degli strumenti che i trader possono utilizzare per prendere decisioni di trading. Non deve essere utilizzato come unico indicatore per decidere se acquistare o vendere.

Open Source

Sorgente Aperto

Livello: base

Argomento: legale

Il software open source è un tipo di software rilasciato sotto una licenza in cui il detentore del copyright concede agli utenti il diritto di studiare, modificare e distribuire il software a chiunque e per qualsiasi scopo. È anche una filosofia che lega gli utenti che credono nella condivisione libera e aperta delle informazioni nel perseguimento di un bene comune più grande.

Ci sono diverse ragioni per cui è importante che un software Bitcoin, ad esempio un wallet, sia rilasciato in open source:

- **Trasparenza**: Il codice sorgente aperto consente a chiunque di esaminare il codice e di verificare che non contenga vulnerabilità o backdoor. Ciò è particolarmente importante per un wallet Bitcoin poiché esso può gestire fondi di valore significativo.
- **Sicurezza**: Il codice aperto consente ai ricercatori di sicurezza e agli sviluppatori di identificare e correggere eventuali vulnerabilità nel software. Ciò aumenta la sicurezza del wallet e dei fondi che esso gestisce.
- **Community**: Il codice aperto consente a una comunità di sviluppatori di contribuire al progetto, di aggiungere nuove funzionalità e di mantenere il software aggiornato. Ciò può aumentare la qualità del software e garantire una maggiore stabilità e affidabilità.
- **Decentralizzazione**: La filosofia del Bitcoin si basa sulla decentralizzazione, sull'open-source e sul libero scambio di informazioni. Avere un wallet open-source contribuisce al principio di decentralizzazione e alle finalità originarie del progetto.

- **Fiducia**: Utilizzare un wallet open-source può creare maggiore fiducia nell'utente poiché esso può verificare il codice sorgente e può essere sicuro che non ci siano parti nascoste o backdoor. Ciò è molto importante per la conservazione dei propri fondi.

In generale l'Open source in questo campo è molto importante poiché garantisce la trasparenza, la sicurezza e la decentralizzazione, tutti elementi fondamentali per una corretta gestione di valuta digitale decentralizzata come Bitcoin.

Ci possono essere diversi livelli con i quali i software Open Source vengono resi disponibili, che possono essere classificati in:

- OSS, usato genericamente come open source, e a volte utilizzato per indicare che non si tratta di FOSS
- FOSS, aggiunge la parola Free che ha diversi significati e traduzioni in italiano
- Reproducible o Riproducibili, per i quali l'utente può creare dal sorgente il programma in autonomia

opt-in

Livello: intermedio

Argomento: legale

Il termine opt-in deriva dal marketing, e si riferisce al fatto che una opzione, o un servizio come l'iscrizione ad una newsletter sia attivata solo a chi ne ha fatto esplicitamente richiesta, contrariamente all'opt-out dove tale opzione viene attivata automaticamente e l'utente se non la vuole deve esplicitare la sua rinuncia.

Un esempio nel caso Bitcoin è l'uso per l'opzione RBF, dove si usa il termine opt-in RBF per differenziarla da Full RBF.

Optimistic Rollup

Livello: avanzato

Argomento: tecnologia

Un "optimistic rollup" è una soluzione di scaling di tipo layer 2 che si basa su calcoli off-chain per registrare in modo affidabile le transazioni che avvengono nel layer 2. Periodicamente, il sistema pubblica una Merkle root delle transazioni che avvengono nel rollup per aggiornare lo "stato" del rollup sulla blockchain sottostante principale. Una rete di validatori esterni controlla le Merkle root per assicurarsi che siano corrette, prima che lo stato venga aggiornato in seguito. Se sorge un'incoerenza, il validatore può pubblicare una prova di frode durante il periodo di contestazione, che può causare il ripristino dello stato del sistema allo stato valido precedente.

Il principale svantaggio degli optimistic rollups rispetto ai rollup a conoscenza zero è il tempo che ci vuole per gli utenti del layer 2 per poter ritirare i loro fondi sulla blockchain sottostante. Poiché un optimistic rollup deve affidarsi a validatori esterni per controllare le Merkle root per "imbrogli" prima che lo stato possa essere aggiornato, è necessario un tempo sufficiente per i validatori per controllare e contestare l'attività che è avvenuta nel layer 2.

Il principale vantaggio degli optimistic rollups rispetto ai loro equivalenti a conoscenza zero è che sono più generalisti e possono supportare smart contract in modo simile alla blockchain sottostante abilitata per lo smart contract. Il supporto nativo per smart contract all'interno del rollup significa che le app possono essere lanciate molto più facilmente, senza la necessità di ulteriori sviluppi.

Options

Opzione

Livello: avanzato

Argomento: finanza

Le opzioni sono contratti finanziari che danno al compratore il diritto, ma non l'obbligo, di acquistare una data quantità di una attività finanziaria sottostante (titoli, indici, valute etc…) ad un determinato prezzo di esercizio chiamato "strike" ad una data specifica o entro tale data. Nel caso in cui l'opzione possa essere esercitata solo alla scadenza avremo opzioni cosiddette "europee", mentre le opzioni "americane" danno al possessore la possibilità di esercizio in qualunque momento entro la data di scadenza.

Oracle

Oracolo

Livello: intermedio

Argomento: tecnologia

All'interno del contesto blockchain, un oracolo è una fonte di dati che viene utilizzata come ponte tra smart contract e altre fonti esterne. Più specificamente, un oracolo è un agente che non solo comunica con origini dati esterne, ma verifica e autentica anche che i dati forniti siano accurati. Pertanto, gli oracoli sono responsabili di fornire informazioni vitali e affidabili ai contratti intelligenti, che a loro volta svolgono determinati compiti. L'importanza degli oracoli si basa sul fatto che gli smart contract sono in grado di accedere solo ai dati contenuti all'interno della blockchain o della propria rete. Pertanto, gli oracoli sono necessari come strumento di comunicazione che "traduca" eventi del mondo reale (dati non deterministici) in valori digitali che possono essere riconosciuti dagli smart contract (dati deterministici).

Order book

Livello: intermedio

Argomento: finanza

Con questo termine ci si riferisce all'insieme degli ordini di acquisto e vendita all'interno di un exchange. Un matching engine effettua l'incontro tra domanda e offerta completando la vendita.

Un order book è una lista attuale di tutti gli ordini aperti per un asset in un dato mercato. L'order book è solitamente pubblico, permettendo ai trader di vedere gli ordini sul mercato. L'order book cambia man mano che i trader aggiungono, rimuovono ed eseguono ordini sul mercato.

Un ordine sull'order book è definito da: direzione, quantità e prezzo limite. Gli order book possono essere usati per valutare preventivamente l'impatto sul mercato di un potenziale ordine. Gli order book forniscono le stesse informazioni di un grafico di profondità, anche se in un formato diverso.

Un order book è la documentazione elettronica dell'attività di acquisto e vendita di un asset su una piattaforma di trading come uno scambio di criptovalute. Generalmente, un order book mostra una visione ordinata di un particolare asset registrando gli ordini di acquisto e di vendita. Le piattaforme che utilizzano gli order book impiegano un motore di corrispondenza per vagliare ed eseguire automaticamente gli ordini di acquisto e di vendita, in tutto o in parte. Un order book comprende diverse informazioni chiave riguardanti un asset. In primo luogo, ha sezioni dedicate agli acquirenti e ai venditori. Poi, c'è una sezione "bid" e "ask". Qui, le "richieste" rappresentano richieste di vendita mentre le "offerte" indicano ordini di acquisto.

Le offerte sono posizionate sulla sinistra mentre le richieste occupano il lato destro del libro. Entrambi i lati hanno prezzi di acquisto e di vendita di vari commercianti. Le offerte sono solitamente rappresentate da un colore verde mentre le richieste sono colorate di rosso.

Tabelle, grafici a linee, grafici a barre e altri metodi di visualizzazione mostrano l'interazione tra acquirenti e venditori. Inoltre, i grafici a candele giapponesi accompagnano un order book per mostrare lo stato attuale e passato del mercato e per aiutare gli operatori a prendere decisioni di trading informate. Nella maggior parte dei casi, gli order book contengono solo ordini impostati per essere eseguiti utilizzando i prezzi specifici di un trader. Questi tipi di ordini sono noti come ordini limite. Gli ordini piazzati per essere eseguiti utilizzando i prezzi correnti di mercato sono chiamati ordini di mercato. I prezzi di offerta più alti e i prezzi di richiesta più bassi appaiono in cima al libro degli ordini. La differenza tra questi due prezzi viene chiamata spread bid-ask. Indica la forza della domanda e dell'offerta.

Order flow

Livello: intermedio

Argomento: finanza

L'order flow è il flusso di ordini di acquisto e vendita di un titolo.

Ordinal

Livello: avanzato

Argomento: tecnologia

Ordinals è un protocollo creato da Casey Rodarmor, che ha lanciato ufficialmente il programma sulla mainnet di Bitcoin il 21 gennaio 2023, che sostanzialmente consente di creare NFT, descritti come "artefatti digitali" sulla Blockchain Bitcoin.

Non è necessario un fork per l'implementazione di questo sistema, che è già disponibile ed è utilizzato.

Nonostante Bitcoin sia fungibile, applicando la teoria degli Ordinal ogni singolo satoshi, o sat, può essere numerato nell'ordine in cui viene minato e questo ordine trasferito dagli input delle transazioni agli output in ordine first-in-first-out, consentendo ad ogni singolo sat esistente di essere Non Fungibile e quindi identificabile univocamente.

Ad ogni singolo sat possono essere associati dati o contenuti arbitrari, creando artefatti digitali unici nativi in Bitcoin; questi contenuti possono essere inseriti direttamente nella blockchain Bitcoin tramite una tecnica chiamata Inscription. L'Inscription avviene inviando i sat in una transazione che rivela il contenuto dell'Inscription on-chain. Le Inscription sono durevoli, immutabili, sicure e decentralizzate come Bitcoin stesso; e i sat ai quali sono associati possono essere conservati nei wallet Bitcoin e trasferiti tramite transazioni Bitcoin, in questo modo è possibile creare degli NFT.

Inserire dati nelle transazioni bitcoin è sempre stato possibile, ma gli Ordinal, nella loro forma attuale, non sarebbero stati possibili senza SegWit e Taproot. Segwit lo ha reso un po' più economico, Taproot ha reso la codifica/decodifica un po' più semplice.

Le Inscription sono state progettate per essere native del web. Le Inscription sono stringhe di byte, identificate con un tipo di contenuto: insieme al contenuto, la transazione Inscription contiene un content type, noto anche come MIME type, che identifica il tipo di contenuto della Inscription: come un'immagine, un testo, un SVG, HTML, CSS, JavaScript, MP3, PNG e JPEG, e possono quindi essere visualizzate in un web browser.

Il contenuto è incluso nel witness della transazione, che normalmente contiene firme e altri dati che provano che una transazione è autorizzata.

Quando viene salvata su blockchain bitcoin, l'Inscription viene associata al primo sat del primo output della transazione, marcandolo in modo permanente, distinta dagli altri sat.

Utilizzando la teoria degli Ordinal, è possibile trovare l'UTXO contenente un'Inscription, e tracciarne i movimenti e la proprietà attraverso il tempo e le transazioni, consentendo di scambiare, regalare, comprare e vendere le Inscription.

Questo permette alle Inscription di essere completamente native in Bitcoin. Possono essere inviate a normali indirizzi bitcoin, in normali transazioni bitcoin, e beneficiare dei timelock, multisig e di altre funzioni Bitcoin.

Le Inscription sono immutabili e on-chain.

La possibilità di salvare NFT o file sulla mainnet Bitcoin ha diviso la comunità Bitcoin sul fatto che possa essere positivo per l'ecosistema Bitcoin, anche in relazione al fatto di occupare lo spazio dei blocchi analogamente a quanto era successo nei primi anni di vita di bitcoin con il progetto BitDNS

Orphan Block

Blocco Orfano

Livello: intermedio

Argomento: tecnologia

Un Orphan Block o Orphaned Bloc, blocco orfano, sarebbe un blocco il cui blocco padre è sconosciuto o inesistente.

Inizialmente questi tipi di blocchi si formavano nelle versioni precedenti del software Bitcoin Core, in cui i nodi di rete potevano ricevere blocchi nonostante la mancanza di dati sui loro antenati.

Dalla versione v.0.10 di Bitcoin Core nel 2015, questo tipo di blocchi orfani di Bitcoin (in senso letterale) non sono più possibili. Tuttavia, il termine Orphan Block è ancora ampiamente utilizzato quando si fa riferimento a blocchi estratti validi che sono stati scartati a seguito di un Reorg, o riorganizzazione della blockchain. Tecnicamente, questi blocchi dovrebbero essere chiamati "blocchi obsoleti" o "blocchi estinti", ma poiché il client denota i loro premi di blocco come "orfani", vengono comunemente indicati come blocchi orfani. Quindi, nonostante abbia un blocco padre noto, la maggior parte delle persone si riferisce a quei blocchi come blocchi orfani piuttosto che blocchi obsoleti.

In una rete blockchain, ci vuole tempo prima che i blocchi vengano trasmessi. Pertanto, due miner dovranno competere se hanno trovato blocchi alla stessa altezza quasi contemporaneamente. Sebbene anche il secondo blocco venga generato durante il normale calcolo, a causa del principio della "catena più lunga", questo blocco creato leggermente dopo il primo non sarà incluso nella chain

principale. Nella rete Bitcoin, tali blocchi dovrebbero essere eliminati completamente e i miner che hanno generato un blocco orfano non riceveranno il block reward, il relativo premio per aver minato il blocco.

OSS

Acronimo di: Open Source Software

Livello: intermedio

Argomento: legale

OSS, Open-Source Software in italiano software con il codice sorgente aperto, è un tipo di software il cui codice sorgente è disponibile al pubblico e può essere modificato e distribuito da chiunque. OSS è spesso distribuito gratuitamente, ma ciò non è necessariamente sempre il caso. L'importante è che il codice sorgente sia disponibile al pubblico e che gli utenti possano modificarlo e distribuirlo senza restrizioni.

Il software OSS si basa su una licenza open source che specifica le condizioni per l'utilizzo, la modifica e la distribuzione del software. Esistono diverse licenze open source, tra cui GPL (General Public License), BSD (Berkeley Software Distribution) e MIT (Massachusetts Institute of Technology) che hanno diverse condizioni su come il software può essere utilizzato e modificato.

Il software OSS è spesso creato e mantenuto da una comunità di sviluppatori, che collaborano tra loro per migliorare il software. Ciò rende OSS particolarmente adatto per progetti complessi, come sistemi operativi e applicazioni aziendali, poiché la comunità può contribuire a trovare e correggere eventuali problemi di sicurezza, a implementare nuove funzionalità e a mantenere il software aggiornato.

Il software OSS è diventato molto popolare negli ultimi anni, e alcuni dei software più diffusi e utilizzati, come Linux, Firefox, e Android sono basati su OSS.

Il software Bitcoin originale è stato rilasciato da Satoshi Nakamoto in Open Source. Molti programmi per Bitcoin sono rilasciati in open-source. La filosofia del Bitcoin si basa sulla decentralizzazione e sull'open-source, quindi è naturale che molti programmi associati a Bitcoin siano rilasciati in open-source.

Dal software originale per Bitcoin si è sviluppato Bitcoin Core, anch'esso rilasciato come open-source e il codice sorgente è disponibile per chiunque sotto la licenza MIT.

Inoltre, ci sono molti wallet Bitcoin open-source disponibili, come Electrum, Mycelium, e Wasabi Wallet. Questi wallet utilizzano il codice sorgente di Bitcoin Core e aggiungono funzionalità supplementari per aiutare gli utenti a gestire le loro chiavi private e i loro fondi Bitcoin in modo sicuro.

In generale, l'utilizzo di open-source per i programmi Bitcoin è importante poiché garantisce la trasparenza, la sicurezza e la decentralizzazione, tutti el-

ementi fondamentali per una corretta gestione di valuta digitale decentralizzata come Bitcoin.

In generale, l'OSS è considerato come una scelta attraente per gli sviluppatori e gli utenti perché offre la possibilità di avere un accesso al codice sorgente, modificarlo, personalizzarlo e distribuirlo senza restrizioni e senza dover pagare costi aggiuntivi.

I OSS e i software liberi FOSS sono simili ma ci sono alcune differenze tra i due.

Il software open source è caratterizzato dal fatto che il codice sorgente è disponibile per chiunque e può essere modificato e distribuito a proprio piacimento. Ciò significa che gli utenti possono esaminare il codice sorgente, apportare modifiche e personalizzare il software in base alle proprie esigenze. In generale, il software open source è creato da una comunità di sviluppatori che lavorano insieme per migliorare il software.

Il software libero, o Free and Open Source Software (FOSS), è simile al software open source, ma c'è una forte enfasi sulla libertà degli utenti di utilizzare, modificare e distribuire il software. Ciò significa che gli utenti possono utilizzare il software per qualsiasi scopo senza restrizioni, e che possono contribuire al miglioramento del software attraverso la modifica del codice sorgente.

In sintesi le differenze tra OSS e FOSS sono:

- OSS si concentra principalmente sulla disponibilità del codice sorgente, e sulla possibilità di modificarlo e distribuirlo.
- FOSS si concentra sulla libertà degli utenti di utilizzare, modificare e distribuire il software.
- In generale entrambi i tipi di software sono gratuiti e spesso i termini OSS e FOSS vengono usati come sinonimi.

Esiste una ulteriore specifica del software OSS e FOSS, che è il software Reproducible, o Riproducibile, che garantisce all'utente non solo di vedere il sorgente e distribuirlo, ma di creare dal sorgente il programma in autonomia.

Ossification

Livello: avanzato

Argomento: politica

In teoria, Bitcoin è qualcosa che può essere aggiornato e cambiato per sempre; finché la supermaggioranza dei partecipanti sceglie di attuare un cambiamento e tutti lo adottano volontariamente e lo applicano, allora Bitcoin può incorporarlo. Bitcoin è tutto sommato un protocollo sul quale si basano i software utilizzati per applicare e interagire con tale protocollo. Qualsiasi modifica arbitraria può essere apportata al protocollo, purché i partecipanti alla comunità Bitcoin siano disposti ad adottarla e a farla rispettare.

Ma in realtà man mano che passa il tempo, diventa sempre più difficile apportare modifiche al protocollo: la comunità Bitcoin è conflittuale, e sulle proposte alla modifica del protocollo ci sono state delle controversie considerate alla stregua di guerre, prima fra tutte la blocksize war, che hanno lasciato il segno. I cambiamenti possono essere considerati dei veri e propri attacchi, che potrebbero essere usati per minare il sistema nel suo complesso.

Questa incrementale resistenza al cambiamento viene definita nella comunità come Ossification, ossificazione in italiano.

L'uso del termine Ossification deriva dal TCP, il protocollo alla base di Internet, per il quale viene evidenziata la difficoltà al cambiamento, a causa dei router che instradano il traffico tra client e server, o tra i nodi più in generale, che sono difficili da aggiornare e rischiano di considerare cattivi o illegali nuove caratteristiche del protocollo o cambiamenti nel comportamento che non erano noti prima, bloccando le connessioni del traffico in transito.

Per alcuni l'ossificazione viene vista come un problema, e il termine ossificazione viene usato con accezione negativa: l'ossificazione si verifica quando un sistema diventa così rigido e inflessibile da non potersi più adattare a nuove condizioni. Luke Dashjr, sviluppatore Bitcoin sin dal 2011 e attore chiave nell'attivazione di Segwit, ha twittato che "L'ossificazione è stupida e suicida".

Per altri l'ossificazione del protocollo Bitcoin è un processo naturale, positivo e auspicabile. E per alcuni addirittura inevitabile: le modifiche al protocollo Bitcoin devono essere affrontate con cautela e conservatorismo, con una dinamica di avvicinamento all'ossificazione.

OTC

Acronimo di: Over-the-Counter

Livello: avanzato

Argomento: finanza

è definita come una transazione effettuata al di fuori di uno exchange, spesso peer-to-peer attraverso scambi privati. Over-the-counter (OTC), chiamato anche off-exchange trading, è una transazione condotta al di fuori di una piattaforma di trading tradizionale, attraverso l'aiuto di intermediari. Spesso, il trading OTC è preferito dai trader privati in quanto di solito comporta enormi transazioni e offre maggiore flessibilità e prezzi migliori rispetto a quelli che possono offrire gli exchange. Equity e derivati su criptovalute sono tra gli strumenti finanziari negoziabili over the counter. Tuttavia, l'OTC non è limitato ai trader privati con grandi disponibilità e il trading over-the-counting è importante anche nelle giurisdizioni in cui, ad esempio, gli scambi di criptovaluta non sono consentiti. Un altro motivo per utilizzare OTC invece di un normale scambio è quando l'importo in questione è così significativo da poter influenzare mercati e prezzo dell'asset crittografico coinvolto. Inoltre, l'over-the-counter è ideale dove

gli strumenti negoziati non sono quotati su una borsa convenzionale. Pertanto, prezzi e quantità coinvolte nelle negoziazioni OTC non sono automaticamente accessibili al pubblico. Notare che le negoziazioni over-the-counter coinvolgono solo due parti. Tuttavia, i commercianti non si incontrano fisicamente. Usano invece reti specifiche per OTC per incontrarsi e commerciare. Il trading over-the-counter è una componente chiave nel settore finanziario globale poiché aumenta la liquidità e migliora la flessibilità del trading. Nonostante i suoi vantaggi, il trading OTC presenta rischi di controparte più elevati rispetto agli scambi formali. L'opzione di trading può soffrire di scarsa liquidità quando sono coinvolti importi di trading elevati. Inoltre, la mancanza di trasparenza sui prezzi porta a condizioni commerciali irregolari. La condivisione delle informazioni sulle reti OTC passa attraverso servizi di elenchi elettronici come l'OTC Bulletin Board (OTCBB). Esempi di reti OTC che trattano Bitcoin e altre criptovalute includono Coinbase Prime, Kraken OTC Desk, BitBay OTC e Bitpanda Plus.

Outbound Liquidity

Livello: avanzato

Argomento: tecnologia

La Outbound Liquidity, o Liquidità in uscita, è la quantità di bitcoin che può essere inviata tramite Lightning Network. L'invio di bitcoin diminuisce la liquidità in uscita di un nodo, mentre la ricezione di bitcoin aumenta la liquidità in uscita del nodo.

L'outbound liquidity è la quantità di fondi che sono disponibili per essere inviati da un dato canale su Lightning Network. In altre parole, si tratta della quantità di denaro che un nodo su Lightning Network è in grado di inviare attraverso uno specifico canale. La quantità può variare nel tempo a seconda delle transazioni che avvengono sulla rete e delle modifiche apportate al canale in questione. L'outbound liquidity è importante perché determina la quantità di fondi che un nodo può inviare in un dato momento e quindi la sua capacità di partecipare alla rete e di eseguire transazioni.

Output Descriptor

Livello: avanzato

Argomento: tecnologia

Gli Output Descriptor, o Output script descriptors, sono stringhe che contengono tutte le informazioni necessarie per consentire a un wallet o a un altro programma di tracciare i pagamenti effettuati o spesi da un particolare script o da un insieme di script correlati (cioè un indirizzo o un insieme di indirizzi correlati, come in un wallet HD).

I Descriptor si combinano bene con miniscript, consentendo a un wallet di gestire il tracciamento e la firma per una maggiore varietà di script. Si combinano bene anche con i PSBT per consentire al wallet di determinare quali chiavi controlla in uno script multisig.

Un Output Descriptor è una stringa di testo che descrive un indirizzo bitcoin e le relative chiavi private. Viene utilizzato principalmente per la gestione dei wallet bitcoin e per facilitare il trasferimento di fondi. Un Output Descriptor può essere utilizzato per rappresentare un singolo indirizzo bitcoin o per rappresentare un intero wallet contenente più indirizzi. In genere, un Output Descriptor è una stringa di testo codificata che può essere facilmente utilizzata dai software per gestire i wallet bitcoin.

Nascono come proposta per rendere più leggibili dall'uomo gli insiemi di scriptPubKeys, insieme a informazioni su come spenderli ("solving"), e opzionalmente anche di chiavi private.

L'obiettivo è quello di risolvere il problema che le chiavi pubbliche, le xpub e le loro versioni a chiave segreta non contengono alcuna informazione sul tipo di script da utilizzare. Storicamente, questo problema è stato affrontato implicando alcuni tipi di script con le chiavi (P2PKH e P2PK, in particolare, e successivamente esteso con P2WPKH e P2SH-P2WPKH).

Tuttavia, questo approccio è:

- **Ambiguo**: l'importazione delle chiavi tra le varie versioni del software può non tenere conto di alcuni script.
- **Non scala bene**: ogni nuovo tipo di script deve essere preso in considerazione per tutte le chiavi, il che influisce negativamente su approcci di filtraggio come BIP37 e BIP157.
- **Non è flessibile**: non c'è un modo semplice per estendere questo sistema alle firme multiple o ad altri script, nonostante questi siano una caratteristica standard in molti software.

L'intento è quello di eliminare del tutto la necessità di importare script e chiavi e di fare in modo che il wallet sia solo un elenco di questi descrittori e dei metadati associati. L'obiettivo è coprire tutti gli script che Bitcoin Core può firmare, essere compatibile con i wallet hardware e BIP174, ed essere facilmente estensibile a nuovi script (comprese le costruzioni multisig più grandi, HTLC, …) e anche ai futuri soft fork che estendono il linguaggio di scripting.

Non è stato progettato per la massima compattezza o per il recupero degli errori. Tuttavia, le proposte per questi ultimi potrebbero essere descritte in termini di syntactic sugar che si traduce nel linguaggio di questa proposta. Inoltre, non include metadati relativi all'uso di uno script, come la data di nascita o il fatto che sia trattato come una modifica o meno.

Output linking

Livello: avanzato

Argomento: tecnologia

Output linking, chiamato anche address reuse, si verifica quando un utente riceve due o più pagamenti alla stessa chiave pubblica o ad altri elementi di script unici. Ciò può accadere perché l'utente riutilizza un indirizzo per ignoranza o come risultato di un bersaglio deliberato, come in un dust attack. I metodi per limitare la perdita di privacy dovuta all'output linking rientrano nella categoria reuse avoidance (evitare il riutilizzo).

Quando si ricevono diversi pagamenti allo stesso indirizzo Bitcoin, gli altri utenti possono ragionevolmente supporre che la stessa persona abbia ricevuto tutti i pagamenti, anche se questi vengono poi spesi attraverso diverse transazioni. Per evitare che terzi facciano tali collegamenti, gli utenti sono incoraggiati a evitare il riutilizzo generando un nuovo indirizzo per ogni pagamento ricevuto.

Purtroppo gli utenti non hanno un controllo completo sui pagamenti che ricevono. In un dust attack, un attaccante invia piccole quantità di bitcoin a indirizzi che sono già apparsi sulla blockchain, producendo un riutilizzo degli indirizzi anche per gli utenti che consapevolmente hanno cercato di evitarlo. Alcuni wallet cercano di risolvere questo problema implementando la coin selection, o coin control, obbligatoria che aiuta a evitare che gli utenti spendano dust nelle transazioni nelle quali vogliono proteggere la loro privacy. Altri wallet offrono funzioni opzionali che consentono di spendere tutte i coin ricevuti allo stesso indirizzo contemporaneamente, ma non più di una volta, eliminando la perdita di privacy derivante dal riutilizzo degli indirizzi con il rischio di non poter spendere i fondi ricevuti a un indirizzo precedentemente utilizzato.

Il riutilizzo degli indirizzi può anche rendere gli utenti di software non funzionanti più vulnerabili agli attacchi di quanto lo sarebbero se non avessero riutilizzato gli indirizzi, come nei casi in cui il software riutilizza i nonce della firma digitale.

Output script descriptors

Livello: avanzato

Argomento: tecnologia

Vedi Output Descriptor

Overbought

Ipercomprato

Livello: intermedio

Argomento: finanza

Quando una criptovaluta è stata acquistata da sempre più investitori nel tempo, con il suo prezzo in aumento per un lungo periodo di tempo. Quando ciò accade senza giustificato motivo, la criptovaluta viene considerata in ipercomprato e si prevede un periodo di vendita.

Oversold

Ipervenduto

Livello: intermedio

Argomento: finanza

Quando una criptovaluta è stata venduta da sempre più investitori nel tempo, con il suo prezzo in calo per un lungo periodo di tempo. Quando ciò avviene senza giustificato motivo, la criptovaluta viene considerata ipervenduta e si prevede un periodo di acquisto.

P2A

Acronimo di: Pay To Anchor

Livello: avanzato

Argomento: tecnologia

Pay To Anchor (P2A) è un nuovo tipo standard di output per witness per le transazioni, basato su un template di output recentemente riconosciuto. Questo consente la creazione di output di ancoraggio senza chiavi, con condizioni di spesa compatte che migliorano l'efficienza rispetto a un output equivalente con sh(OP_TRUE), oltre a garantire la stabilità del txid della transazione di spesa. Nota: la propagazione della spesa di questo tipo di output sulla rete sarà limitata fino a quando un numero sufficiente di nodi non adotterà questo aggiornamento.

P2C

Acronimo di: Pay-to-Contract

Livello: avanzato

Argomento: tecnologia

Pay-to-Contract (P2C) è un metodo per modificare le chiavi pubbliche Bitcoin che è stato descritto per la prima volta nel 2012, ma di cui non si parla molto. Consente di ricevere denaro su un commitment privato che può essere mantenuto segreto per sempre o dimostrato pubblicamente in seguito.
È semplice quanto potente.

I protocolli pay-to-contract consentono a chi spende e a chi riceve di concordare il testo di un contratto (o qualsiasi altra cosa) e quindi creare una chiave pubblica con un commit su quel testo. Chi spende può quindi successivamente dimostrare

che il pagamento con il commit su quel testo e che sarebbe stato computazionalmente impossibile assumere tale commit senza la cooperazione del destinatario. In breve, P2C consente a chi spende di dimostrare a un tribunale o al pubblico per cosa ha pagato.

È un protocollo di pagamento elettronico per le tipiche relazioni cliente-commerciante che non richiede l'invio di un descrittore di pagamento affidabile (firmato) da parte del commerciante al cliente. Invece, il numero del "conto" di destinazione per il pagamento viene creato esclusivamente sul lato del cliente. Ciò elimina la necessità di qualsiasi comunicazione criptata o autenticata nel protocollo e lo rende sicuro anche se l'infrastruttura online del commerciante viene compromessa. Inoltre, la transazione di pagamento stessa funge da ricevuta con timestamp per il cliente. Prova cosa è stato pagato e chi ha ricevuto i fondi, sempre senza affidarsi a firme del commerciante. In particolare, fondi e ricevuta vengono scambiati in un'unica azione atomica. La natura asimmetrica della relazione cliente-commerciante è fondamentale.

Il protocollo è specificamente progettato pensando a Bitcoin come sistema di pagamento di base. Ciò ha l'utile vantaggio che tutte le transazioni sono pubbliche. Tuttavia, l'unico requisito essenziale per il sistema di pagamento è che gli "account" siano coppie di chiavi arbitrarie create dall'utente di un criptosistema le cui coppie di chiavi godono di una proprietà omomorfa. Tutti i criptosistemi di tipo ElGamal hanno questa caratteristica.

P2EP

Acronimo di: Pay-to-Endpoint

Livello: avanzato

Argomento: tecnologia

Vedi PayJoin

P2MS

Acronimo di: Pay-To-Multisig

Livello: avanzato

Argomento: tecnologia

P2MS (Pay To Multisig) è un tipo di transazione Bitcoin che permette di vincolare Bitcoin a più chiavi pubbliche, richiedendo le firme di alcune o tutte queste chiavi per sbloccarli.

Un output P2MS specifica un numero N di chiavi pubbliche e richiede almeno M firme valide per autorizzare una transazione (M-di-N). Ad esempio, è possibile creare uno script P2MS che includa le chiavi pubbliche di tre persone diverse, ma solo due di loro devono fornire le rispettive firme per spendere i Bitcoin.

P2MS è stato uno dei primi metodi per implementare transazioni multisig in Bitcoin, ma non è mai stato molto utilizzato. Presenta infatti alcuni svantaggi, tra cui:

- Costi di transazione elevati: le transazioni P2MS sono più grandi delle transazioni standard, il che comporta costi di transazione maggiori.

- Privacy limitata: lo script P2MS completo è visibile sulla blockchain, il che può rivelare informazioni sulle parti coinvolte nella transazione.

Per questi motivi, P2MS è stato in gran parte sostituito da P2SH che consente di "nascondere" lo script completo all'interno di un hash, riducendo i costi di transazione e migliorando la privacy.

P2P

Acronimo di: Peer-to-Peer

Livello: base

Argomento: tecnologia

Il termine p2p o Peer-to-peer sta ad indicare un modello di architettura logica di rete informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di client o server fissi, ma sotto forma di nodi paritari (peer), potendo fungere al contempo da client e server verso gli altri nodi terminali (host) della rete.

I computer che partecipano alla rete p2p sono tra loro pari, sono tutti uguali, non ci sono nodi "speciali" e tutti i nodi condividono l'onere di fornire servizi di rete. I nodi della rete si interconnettono in una rete a maglie con una topologia "piatta". Non c'è un server, né un servizio centralizzato, né una gerarchia all'interno della rete. I nodi di una rete P2P forniscono e consumano servizi allo stesso tempo, con la reciprocità che funge da incentivo alla partecipazione. Le reti P2P sono intrinsecamente resilienti, decentralizzate e aperte. Un esempio preminente di architettura di rete P2P è stata la prima Internet, dove i nodi della rete IP erano uguali. Oggi l'architettura di Internet è più gerarchica, ma il protocollo Internet conserva ancora la sua essenza di topologia piatta. Oltre a bitcoin, l'applicazione più vasta e di maggior successo delle tecnologie P2P è la condivisione di file, con Napster come pioniere e BitTorrent come evoluzione più recente dell'architettura.

Bitcoin è strutturato come un'architettura di rete p2p su Internet.

Nel caso di Bitcoin, la rete è costruita in modo che ogni utente trasmetta le transazioni a tutti i nodi della rete, permettendo a tutti di controllare la validità delle transazioni: quindi non è necessario nessun ente centrale.

L'architettura di rete P2P di Bitcoin è molto più di una scelta topologica. Bitcoin è un sistema di denaro digitale P2P per concezione, e l'architettura di rete è sia un riflesso che un fondamento di questa caratteristica fondamentale. La

decentralizzazione del controllo è un principio di progettazione fondamentale che può essere raggiunto e mantenuto solo da una rete di consenso P2P piatta e decentralizzata.

Il termine "rete bitcoin" si riferisce all'insieme dei nodi che eseguono il protocollo P2P bitcoin. Oltre al protocollo bitcoin P2P, esistono altri protocolli, come Stratum, utilizzati per il mining e per wallet leggeri o mobili. Questi protocolli aggiuntivi sono forniti da server di routing gateway che accedono alla rete bitcoin utilizzando il protocollo bitcoin P2P e poi estendono la rete ai nodi che eseguono altri protocolli. Ad esempio, i server Stratum collegano i nodi di mining Stratum tramite il protocollo Stratum alla rete bitcoin principale e collegano il protocollo Stratum al protocollo bitcoin P2P. Utilizziamo il termine "rete bitcoin estesa" per riferirci alla rete complessiva che comprende il protocollo P2P bitcoin, i protocolli di pool-mining, il protocollo Stratum e qualsiasi altro protocollo correlato che colleghi i componenti del sistema bitcoin.

P2PK

Acronimo di: Pay-to-Public-Key

Livello: intermedio

Argomento: tecnologia

P2PK, Pay-to-Public-Key in italiano *Paga alla Chiave pubblica*, è il primo e più semplice metodo di pagamento su Bitcoin.

Si tratta di un tipo di ScriptPubKey (o locking script) che vincola la spesa dei bitcoin a una chiave pubblica specifica.

In questo caso, il pagamento non viene effettuato a un "indirizzo Bitcoin", ma direttamente a una chiave pubblica.

Storia e deprecazione P2PK è stato introdotto da Satoshi Nakamoto nella prima versione di Bitcoin, ma è stato rapidamente deprecato a favore di P2PKH. Quest'ultimo migliora la sicurezza e la privacy, sostituendo la chiave pubblica in chiaro con il suo hash.

Funzionamento Una transazione P2PK è una transazione in cui gli input utilizzano la chiave pubblica in chiaro.
Ad esempio, se Alice invia 1 BTC a Bob in una transazione P2PK, include direttamente la chiave pubblica di Bob nella transazione. Per spendere questi bitcoin, Bob dovrà fornire una firma digitale generata con la sua chiave privata corrispondente.

La chiave pubblica, derivata dalla chiave privata tramite crittografia a curva ellittica, può essere rappresentata in diversi formati:

- **Compressa** (33 byte): contiene solo la coordinata x con un prefisso che indica la parità della coordinata y

- **Non compressa** (65 byte): contiene sia la coordinata x che y

Prefisso	Contiene	Lunghezza (byte)	y	formato compresso
02	x	33	pari	sì
03	x	33	dispari	sì
04	x, y	65		no

Essendo la curva ellittica simmetrica rispetto all'asse x, nel formato compresso si memorizza solo x con l'indicazione della parità di y.

Lo script ScriptPubKey P2PK ha la seguente forma:

```
<Chiave pubblica da inviare> OP_CHECKSIG
```

Per sbloccare i fondi, il destinatario deve fornire una firma digitale valida, inserita nello scriptSig:

```
<SIGNATURE> (Firma digitale valida)
```

Un esempio dell'uso di P2PK è nella prima transazione Bitcoin, fatta il 12 gennaio 2009 da Satoshi a Hal Finney, presente nel blocco 170.

Satoshi stesso decise di abbandonare P2PK al posto di P2PKH per due motivi:

- La crittografia a curva ellittica è vulnerabile a una versione modificata dell'algoritmo di Shor, che può risolvere il problema del logaritmo discreto sulle curve ellittiche. In parole semplici, ciò significa che in futuro un computer (es. quantistico) potrebbe essere in grado di ricavare una chiave privata partendo da una chiave pubblica. Pubblicando la chiave pubblica solo quando le monete vengono spese (e assumendo che gli indirizzi non vengano riutilizzati), un attacco di questo tipo diventa inefficace.
- Poiché l'indirizzo è più piccolo (20 byte) della chiave pubblica, è più facile da stampare e più semplice da incorporare in supporti di archiviazione ridotti, come i codici QR.

P2PK è l'indirizzo che si vede più spesso nelle transazioni coinbase dei primi blocchi della blockchain. Ciò è dovuto al fatto che il miner originale Bitcoin Core utilizzava P2PK per la ricompensa di blocco quando creava nuovi blocchi.

P2PKH

Acronimo di: Pay-to-Public-Key-Hash

Livello: intermedio

Argomento: tecnologia

Pay-to-Public-Key-Hash (P2PKH) è un tipo di transazione che è stato disponibile fin dall'inizio di Bitcoin e apparve per la prima volta sulla blockchain meno

di due settimane dopo il blocco di genesi.
Rispetto a P2PK, Pay-to-Public-Key, P2PKH introduce miglioramenti significativi, come l'uso di un indirizzo. Gli indirizzi contengono un checksum, che aiuta a prevenire errori di battitura e la perdita di bitcoin.

Gli indirizzi P2PKH sono solitamente lunghi tra i 33 e i 34 caratteri (ma possono arrivare a un minimo di 26) e sono codificati nel formato Base58. Iniziano con il prefisso "1".

La creazione di un indirizzo P2PKH prevede l'applicazione delle funzioni di hash SHA-256 e RIPEMD-160 su una chiave pubblica.
Questo processo riduce la quantità di dati, contribuendo a risparmiare spazio nel blocco e a diminuire le commissioni di transazione. Inoltre, aumenta la sicurezza contro l'ingegneria inversa della chiave privata, oltre alla già consolidata protezione offerta dalla curva ellittica secp256k1.

P2PKH: Funzionamento e Vantaggi P2PKH, ovvero "Pay-to-Public-Key-Hash", consente di spendere bitcoin attraverso l'hash di una chiave pubblica. Si tratta del primo tipo di indirizzo Bitcoin, noto anche come Legacy, che inizia con "1" e può variare da 26 a 36 caratteri, ad esempio:

```
1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
```

Questa tipologia di indirizzi ha sostituito P2PK, che utilizzava direttamente la chiave pubblica, apportando maggiore sicurezza. Con l'introduzione di SegWit gli indirizzi P2PKH hanno perso popolarità, ma rimangono fondamentali per comprendere il funzionamento degli script Bitcoin. Le commissioni medie per le transazioni da un indirizzo P2PKH sono più alte rispetto a quelle di SegWit, poiché le transazioni legacy occupano più spazio nei blocchi.

Esempio di Transazione P2PKH In una transazione P2PKH, gli input vengono bloccati tramite lo ScriptPubKey P2PKH. L'hash della chiave pubblica funge da indirizzo, rendendo P2PKH uno dei tipi di script più comuni.
Per esempio, se Alice vuole inviare 1 BTC a Bob, quest'ultimo fornisce un indirizzo del suo wallet ad Alice, che lo include nella transazione. Quando Bob vorrà spendere i bitcoin ricevuti, dovrà firmare la transazione con la chiave privata associata alla chiave pubblica il cui hash è presente nella transazione di Alice.

Lo script di blocco P2PKH include l'hash della chiave pubblica e utilizza i seguenti opcode:

```
OP_DUP OP_HASH160 <indirizzo> OP_EQUALVERIFY OP_CHECKSIG
```

Per risolvere lo script, il proprietario dell'indirizzo deve fornire la chiave pubblica originale e una firma valida.

Vantaggi di P2PKH rispetto a P2PK Satoshi Nakamoto decise di adottare P2PKH al posto di P2PK per due motivi principali:

- Maggiore sicurezza contro attacchi futuri: La crittografia a curva ellittica (ECC), usata per le chiavi pubbliche e private, potrebbe essere vulnerabile a un futuro attacco con computer quantistici in grado di risalire alla chiave privata dalla chiave pubblica. Con P2PKH, la chiave pubblica viene rivelata solo al momento della spesa, riducendo il rischio di esposizione.
- Maggiore efficienza: L'hash di una chiave pubblica è più piccolo (20 byte), facilitandone la stampa e l'incorporazione in supporti ridotti come i codici QR.

P2SH

Acronimo di: Pay-to-Script-Hash

Livello: intermedio

Argomento: tecnologia

Pay-to-Script-Hash (P2SH) è un tipo di locking script, o ScriptPubKey, che consente di spendere i bitcoin attraverso uno script il cui hash è specificato all'interno della transazione.

Introdotto nel 2012 e attivato nel 2013, ha aggiunto un nuovo modo con il quale possono essere validate le transazioni. È più comunemente identificabile tramite gli indirizzi Bitcoin che iniziano con un "3" rispetto al precedente formato nel quale iniziavano per "1".

Una transazione P2SH è una transazione i cui gli UTXO in input sono stati bloccati utilizzando una ScriptPubKey P2SH.

Il suo uso più frequente è quello di creare dei pagamenti multisig, ovvero che per essere spesi richiedono più firme all'interno di un insieme di firme definite. Nel caso 2 su 3, su 3 firme preimpostate è necessario che venga firmata con 2 firme.

Ad esempio, se Alice invia a Bob 1 BTC in una transazione P2SH, include l'hash dello script necessario per spendere il bitcoin nella transazione. Questo script può richiedere le firme delle chiavi private di Bob e altri requisiti. Quando Bob vuole spendere il bitcoin che ha ricevuto da Alice, ricostruisce lo script il cui hash Alice ha usato per inviare il bitcoin e firma la transazione con le chiavi private richieste dallo script.

P2SH è estremamente flessibile perché consente agli utenti di costruire script arbitrari.

P2SH viene utilizzato per abilitare la retrocompatibilità con i nuovi tipi di transazione, incluso P2WSH di SegWit, e a volte i due vengono indicati insieme con la notazione P2SH-P2WSH.

Inoltre, non è necessario che il mittente della transazione conosca il tipo di script a cui sta inviando. Nell'esempio precedente, Bob può costruire privatamente lo

script che vuole usare e inviare ad Alice solo l'hash di quello script, in questo modo viene garantita una maggiore privacy per Bob.

Lo standard delle transazioni P2SH è definito nel BIP 16.

P2TR

Acronimo di: Pay-to-Taproot

Livello: avanzato

Argomento: tecnologia

P2TR (Pay-to-Taproot, paga a Taproot), noto anche come indirizzo Taproot o Bech32m, è il formato di indirizzo bitcoin più recente e avanzato. Taproot introduce sicurezza, privacy, flessibilità e scalabilità più avanzate in bitcoin.

Gli indirizzi di taproot iniziano con **bc1p** e non fanno distinzione tra maiuscole e minuscole.

I vantaggi di Taproot includono la possibilità di utilizzare le firme Schnorr, che offrono una maggiore sicurezza, fee più basse e transazioni multi-key più flessibili. Gli indirizzi a più chiavi che utilizzano P2TR hanno lo stesso aspetto di quelli a chiave singola, il che garantisce agli utenti della multi-key una maggiore privacy. Taproot consente anche uno scripting più avanzato chiamato tapscript, che permette di costruire smart contract più complessi su bitcoin.

P2TR è un tipo di ScriptPubKey che blocca i bitcoin su uno script che può essere sbloccato da una chiave pubblica o da un MAST (Merkelized Alternative Script Tree), consentendo ai bitcoin di essere spesi in vari modi.

In apparenza, un'uscita P2TR blocca i bitcoin a una singola chiave pubblica Schnorr, ma questa chiave pubblica è in realtà l'aggregazione di una chiave pubblica P e di un'altra chiave pubblica calcolata dal Merkle root di una lista di altre ScriptPubKey.

I bitcoin in un output P2TR possono essere spesi pubblicando una firma per la chiave pubblica P, oppure soddisfacendo uno degli script contenuti nel Merkle tree. La prima opzione è chiamata key path, mentre la seconda opzione è chiamata script path.

Pay-to-Taproot combina le funzionalità degli script P2SH (Pay-to-Script-Hash) e P2PK (Pay-to-Public-Key) in modo flessibile, permettendo al proprietario o ai proprietari di scegliere come spendere i propri Bitcoin. Ciò rende il P2TR un miglioramento significativo per la privacy degli utenti.

Sebbene esistano molti modi per spendere un output P2TR, deve essere rivelato solo quello utilizzato, permettendo alle alternative non utilizzate di rimanere private. Inoltre, grazie all'aggregazione delle chiavi di Schnorr, la chiave pubblica P può essere essa stessa una chiave aggregata, che può rappresentare una configurazione multisig. Soprattutto, lo stato della chiave pubblica P come chiave

multisig o come chiave singola non viene mai rivelato, e quindi tutti gli output di P2TR si assomigliano, vanificando molte euristiche di Chain analysis e preservando la privacy degli utenti.

Pay-to-Taproot è un'output SegWit versione 1, il che significa che le firme per gli input P2TR sono memorizzate nel Witness di una transazione, non nello ScriptSig. Come altri indirizzi SegWit, gli indirizzi P2TR utilizzano la codifica Bech32.

P2WPKH

Acronimo di: Pay-to-Witness-Public-Key-Hash

Livello: avanzato

Argomento: tecnologia

Gli indirizzi P2WPKH (Pay to Witness Public Key Hash, paga all'hash del witness di una chiave publica) sono di solito indicati come indirizzi "SegWit nativi" o *Native SegWit*, sono indirizzi che iniziano con **bc1q** e sono il tipo di indirizzo più comunemente utilizzato dai moderni wallet bitcoin, per la loro capacità di costruire transazioni che occupando meno spazio rispetto agli indirizzi legacy, consentono all'utente di risparmiare sulle fee.

P2WPKH è un tipo di ScriptPubKey che viene utilizzato per bloccare bitcoin su un indirizzo Segwit. Una transazione P2WPKH è simile a una transazione P2PKH in molti modi; blocca comunque i bitcoin sull'hash di una chiave pubblica. La differenza principale è che P2WPKH utilizza SegWit. Ciò significa che ScriptSig, lo script che sblocca il bitcoin, per tutti gli input viene spostato al di fuori del corpo della transazione e nella sezione Witness e chiamato Script Witness. Questi dati sono ancora registrati sulla blockchain, ma i dati comportano fee inferiori rispetto ai dati normali, rendendo le transazioni SegWit più economiche delle transazioni legacy.

P2WSH

Acronimo di: Pay-to-Witness-Script-Hash

Livello: avanzato

Argomento: tecnologia

P2WSH è un tipo di transazione simile a una transazione P2SH sotto diversi punti di vista, tranne per il fatto che utilizza SegWit.

Come una transazione P2SH, una transazione P2WSH blocca bitcoin sull'hash di uno script.

Per spendere questi bitcoin, lo spender deve presentare lo script, chiamato RedeemScript, e tutte le firme richieste. A livello tecnico, P2WSH descrive effettivamente la ScriptPubKey che viene utilizzata per bloccare bitcoin su un

hash di script SegWit. Una transazione P2WSH spende i bitcoin che erano precedentemente bloccati su un indirizzo P2WSH.

Poiché P2WSH è una transazione SegWit, quando un output P2WSH viene utilizzato come input, lo ScriptSig viene spostato nella sezione Witness e chiamato WitnessScript.

Finché non viene speso un UTXO P2SH-P2WPKH e non viene esposto il RedeemScript, un indirizzo P2SH-P2WPKH è indistinguibile da un indirizzo P2SH non segwit (come un indirizzo multi-firma non segwit).

Package relay

Livello: avanzato

Argomento: tecnologia

Il Package relay è una funzionalità proposta per i nodi relay Bitcoin che consentirebbe loro di inviare e ricevere pacchetti di transazioni correlate che verrebbero accettate o rifiutate in base al feerate del pacchetto complessivo, anziché far accettare o rifiutare ogni singola transazione del pacchetto solo in base al proprio feerate.

Senza il Package relay, non è possibile far pagare una transazione che sia al di sotto del feerate minimo accettato dai nodi. I nodi rifiuteranno la transazione genitore per il suo feerate troppo basso e poi ignoreranno la transazione figlio con fee bump perché la transazione genitore è necessaria per convalidare la transazione figlio. Questo è particolarmente problematico perché il feerate minimo che un nodo accetta dipende dal contenuto della sua mempool, quindi una transazione genitore che in precedenza poteva essere sottoposta a fee bump potrebbe non esserlo più. Questo ha implicazioni significative per la sicurezza di Lightning Network e di altri protocolli contrattuali sensibili al tempo che vogliono dipendere dal fee bumping di CPFP.

L'ostacolo principale all'aggiunta del supporto per il Package relay al protocollo P2P Bitcoin è garantire che un'implementazione non crei nuovi vettori per attacchi denial-of-service.

Panic Selling

Livello: base

Argomento: finanza

È una vendita su larga scala da parte di molti utenti che provoca una reazione a catena con conseguente un forte calo dei prezzi. Gli investitori in questi casi effettuano vendite con poco riguardo al prezzo sotto la spinta emotiva della paura, nella speranza di non aggravare ulteriormente le proprie perdite.

Paper wallet

Livello: intermedio

Argomento: tecnologia

Una soluzione di cold storage, per conservare le criptovalute in ambiente offline.

Il paper wallet, letteralmente *portafoglio cartaceo*, è così chiamato poiché si riferisce alla pratica di stampare la chiave privata, sotto forma di QR Code o frase mnemonica: quando gli utenti desiderano accedere ai loro fondi, devono scansionare il loro paper wallet, digitare/importare la propria chiave privata.

I paper wallet non sono in realtà wallet, ma piuttosto chiavi private e indirizzi stampati su carta. Sebbene le chiavi e gli indirizzi possano tecnicamente essere generati in modo non deterministico o deterministico, l'usabilità è fondamentalmente uguale o inferiore a quella di un wallet software non deterministico. I paper wallet presentano una serie di svantaggi significativi, tra cui l'incoraggiamento all'Address reuse, l'esposizione delle chiavi a dispositivi di rete poco protetti (le stampanti) e la mancata gestione dei cambi di indirizzo. I paper wallet non devono essere confusi con i recovery seed.

passphrase

Livello: base

Argomento: tecnologia

In Bitcoin, la passphrase è una parola o una frase opzionale che può essere aggiunta alla frase mnemonica o alla chiave privata per aumentare la sicurezza del wallet. La frase mnemonica è una sequenza di 12 o 24 parole che viene generata casualmente quando si crea un wallet Bitcoin. Questa frase mnemonica è necessaria per accedere ai fondi del wallet.

La passphrase funziona combinandosi con la frase mnemonica per generare una nuova seed, che è una stringa di dati alfanumerici che viene utilizzata per generare le chiavi private e pubbliche del wallet. Se qualcuno conosce la frase mnemonica, ma non la passphrase, non sarà in grado di accedere ai fondi del wallet.

Il funzionamento della passphrase è descritto:

- nel BIP 38 Passphrase-protected private key
- nel BIP 39 Mnemonic code for generating deterministic keys

La passphrase offre diversi vantaggi di sicurezza:

- Aumenta la complessità della seed, rendendo più difficile per gli hacker crackarla.
- Fornisce un'ulteriore layer di sicurezza in caso la frase mnemonica venga compromessa.
- Permette di creare wallet nascosti, che non sono visibili se non si conosce la passphrase.

È importante scegliere una passphrase complessa e difficile da indovinare. Si consiglia di utilizzare una combinazione di lettere, numeri e simboli. La passphrase non deve essere memorizzata insieme alla frase mnemonica.

Ecco alcuni suggerimenti per scegliere una passphrase sicura:

- Usa una combinazione di lettere, numeri e simboli.
- Non usare parole o frasi comuni.
- Non usare informazioni personali, come il tuo nome, la tua data di nascita o il tuo indirizzo.
- Crea una passphrase che sia facile da ricordare, ma difficile da indovinare.

Se stai cercando un modo per migliorare la sicurezza del tuo wallet Bitcoin, la passphrase è un'opzione da considerare.

pathfinding

Livello: avanzato

Argomento: tecnologia

Quando viene effettuato un pagamento sulla rete Lightning Network, il pagamento deve attraversare uno o più canali dal nodo del mittente del pagamento a quello del destinatario.

La ricerca del percorso dal mittente al destinatario è un processo chiamato Pathfinding. Poiché l'instradamento viene effettuato dal mittente, quest'ultimo deve trovare un percorso adeguato per raggiungere la destinazione.

Pathfinding (la ricerca del percorso), path selection (la selezione del percorso), MPP multipart payments (i pagamenti multiparte) e il ciclo di tentativi di pagamento per tentativi ed errori occupano la maggior parte del livello di pagamento nella parte superiore della suite del protocollo Lightning.

Il termine pathfinding può essere un po' fuorviante, perché suggerisce che venga ricercato un unico percorso che colleghi due nodi.

Se il mittente e il destinatario sono collegati ad altri nodi ben connessi e dispongono di almeno un canale con capacità adeguata, ci saranno migliaia di percorsi. Il problema diventa selezionare il percorso migliore che riuscirà a consegnare il pagamento, tra migliaia di percorsi possibili.

Per selezionare il percorso migliore, dobbiamo innanzitutto definire cosa intendiamo per "migliore".

I criteri possono essere molti e diversi, come ad esempio:

- Percorsi con sufficiente liquidità. Ovviamente, se un percorso non ha abbastanza liquidità per instradare il nostro pagamento, non è un percorso adatto.
- Percorsi con fee basse. Se abbiamo diversi candidati, potremmo voler selezionare quelli con fee più basse.

- Percorsi con timelock brevi. Potremmo voler evitare di bloccare i nostri fondi per troppo tempo e quindi selezionare percorsi con timelock più brevi.

Non c'è certezza sul bilanciamento dei canali: se conoscessimo gli esatti balance di ogni canale, potremmo calcolare uno o più percorsi di pagamento usando uno qualsiasi degli algoritmi standard di pathfinding. Ma non conosciamo i balance dei canali; conosciamo solo la capacità aggregata dei canali, che viene comunicata dai nodi. Affinché un pagamento abbia successo, deve esserci un balance adeguato sul lato di invio del canale. Se non sappiamo come è distribuita la capacità tra i partner del canale, non sappiamo se c'è un balance sufficiente nella direzione in cui stiamo cercando di inviare il pagamento.

I balance non vengono annunciati negli aggiornamenti del canale per due motivi: privacy e scalabilità. In primo luogo, l'annuncio dei balance ridurrebbe la privacy della Lightning Network, perché consentirebbe di sorvegliare i pagamenti attraverso l'analisi statistica delle variazioni dei balance. In secondo luogo, se i nodi annunciassero i balance (a livello globale) a ogni pagamento, la scalabilità della Lightning Network sarebbe pari a quella delle transazioni Bitcoin on-chain, che vengono trasmesse a tutti i partecipanti. Pertanto, i balance non vengono annunciati.

Il nodo Lightning crea una lista di percorsi candidati, li filtra e li ordina in base ad alcuni parametri (ad esempio tenendo conto dei nodi attraverso i quali ha già inviato pagamenti con successo) e li prova in sequenza. Se tutti i nodi si comportano bene, verificare di un singolo percorso dovrebbe essere veloce (~ 1 secondo) indipendentemente dalla dimensione della rete, ma se i nodi non si comportano bene, il tempo di verifica può crescere esponenzialmente.

Calcolare il percorso più economico può essere una funzione complicata, e Rene Pickhardt e Stefan Richter hanno effettuato uno studio che ha rilevato che, se nella funzione di pagamento è inclusa una base_fee maggiore di 0, la complessità di questo calcolo è tale da poter essere definito un problema NP-completo (nella teoria della complessità computazionale i problemi NP-completi sono i più difficili problemi nella classe NP "problemi non deterministici in tempo polinomiale").

Per questo motivo è nata l'iniziativa Zero Base Fee, che promuove l'impostazione base_fee a 0 per migliorare le prestazioni di Lightning Network, consentendo di effettuare anche pagamenti per importi che senza tale impostazione hanno alte probabilità di fallire.

Patoshi Pattern

Livello: intermedio

Argomento: tecnologia

Il "Patoshi Pattern" è un concetto introdotto da Sergio Demian Lerner nel

2013, e approfondito in seguito dallo stesso Lerner e altri ricercatori.
Si tratta di un comportamento nel mining individuato nei primi blocchi della blockchain di Bitcoin, che suggerisce che una singola entità, denominata "Patoshi," abbia minato oltre 1 milione di Bitcoin nei suoi primi 12 mesi di esistenza. Questa teoria si basa su analisi tecniche delle prime transazioni e dei modelli di nonce utilizzati nei blocchi.

L'attribuzione del Patoshi Pattern a Satoshi Nakamoto è controversa per diverse ragioni. Prima di tutto, la simmetria temporale tra il comportamento di mining di Patoshi e lo sviluppo iniziale del protocollo Bitcoin porta molti a credere che dietro questa attività ci sia proprio Nakamoto ma il fatto che nessuno sappia chi sia realmente Satoshi Nakamoto rende qualsiasi attribuzione speculativa. Non ci sono prove definitive che colleghino direttamente Patoshi a Nakamoto.

Inoltre non vi è mai stata alcuna movimentazione evidente di questi fondi, a parte una specifica transazione nota, il che alimenta ulteriormente il mistero. Inoltre, l'identificazione precisa degli indirizzi di Nakamoto è complicata dalla natura anonima della blockchain e dalla mancanza di prove concrete che colleghino direttamente Nakamoto al Patoshi Pattern.

Questa ambiguità lascia spazio a speculazioni sul fatto che il Patoshi Pattern possa rappresentare l'attività di uno o più miner diversi da Satoshi, oppure che possa trattarsi di una sofisticata organizzazione di mining coordinata. Queste teorie sono ulteriormente complicate dall'apparente immobilità del tesoro di Bitcoin associato a questo pattern, che continua ad attirare interesse e curiosità nella comunità Bitcoin e contribuiscono ad alimentare il dibattito e la speculazione sulla sua vera identità e sul suo ruolo nella creazione e nello sviluppo di Bitcoin.

Sergio Demian Lerner ha attirato per la prima volta l'attenzione su questo fenomeno nel 2013. L'analisi di Lerner stimava che il miner Patoshi avrebbe potuto accumulare circa 1 milione di bitcoin.
Jameson Lopp, co-fondatore di Casa, ha ampliato questo lavoro nel 2022, notando che il miner Patoshi non sembrava massimizzare la redditività: "Sembra che questo miner fosse più concentrato sul mantenimento della stabilità della rete piuttosto che sul guadagno personale", ha osservato Lopp.
"Questo misterioso schema di mining offre uno sguardo affascinante sui primi giorni di Bitcoin", ha affermato Adam Back, CEO di Blockstream e rinomato crittografo, "Suggerisce che Satoshi stava probabilmente prendendo misure per proteggere la giovane rete dalle vulnerabilità".
Dettagli selettivi della blockchain indicano che il miner Patoshi avrebbe spesso ridotto la potenza di hash quando altri minatori si univano alla rete, probabilmente per promuovere la decentralizzazione. Ci sono stati anche periodi in cui questo miner ha sospeso l'attività, portando a speculazioni sul fatto che Satoshi stesse testando la resilienza della rete contro potenziali attacchi.

A febbraio 2025 Arkham ha aggiunto ulteriori 22.000 indirizzi associati al Patoshi Pattern, portando ad un totale di 1.096.354 i bitcoin associati a questi

indirizzi.

PayJoin

Livello: avanzato

Argomento: tecnologia

PayJoin, noto anche come **P2EP** Pay-to-Endpoint, è un tipo speciale di transazione Bitcoin CoinJoin tra due parti in cui una parte paga l'altra, in cui sia il mittente che il destinatario contribuiscono con gli input al fine di rompere l'euristica della proprietà comune degli input, Common Input Ownership Heuristic, un'ipotesi utilizzata per togliere la privacy agli utenti Bitcoin.

Questo tipo di coinjoin ha proprietà di privacy diverse, probabilmente migliori.

La transazione non ha la caratteristica di avere più output con lo stesso valore e quindi non è ovviamente visibile come una CoinJoin con output uguali.

L'euristica della proprietà comune degli input è una delle euristiche più utilizzate nella chain analysis. Presuppone che, in una determinata transazione, tutti gli input siano stati firmati dalla stessa entità. Fino ad oggi, questa è stata un'ipotesi relativamente sicura, dato che l'uso del multisig rimane basso. La proposta P2EP è stata creata per rompere questo presupposto e migliorare la privacy di Bitcoin.

Ad esempio, se un utente riceve un pagamento a un indirizzo P2PKH e poi spende questo output per creare due output, uno a un indirizzo P2SH e uno a un indirizzo P2PKH, si può presumere che l'output P2SH appartenga ora a un'altra parte, mentre l'output P2PKH è un output di modifica e appartiene ancora al mittente.

Sebbene la sintassi di P2EP assomigli ai numerosi tipi di script di Bitcoin, P2EP non è uno script. Si tratta piuttosto di un protocollo che consente a due utenti di Bitcoin di effettuare transazioni in modo da preservare la privacy. Utilizzando un canale peer-to-peer, come un indirizzo onion, un mittente e un destinatario possono scambiarsi informazioni sugli UTXO che desiderano utilizzare come input in una transazione.

Possono quindi costruire e firmare in modo cooperativo la transazione utilizzando PSBT, Partially Signed Bitcoin Transaction o Transazione Bitcoin parzialmente firmata definito nel BIP 174. La transazione risultante assomiglierà semplicemente a una transazione di tipo "azionario". La transazione risultante sarà semplicemente simile a una tipica transazione con più ingressi e più uscite.

Payment Channel

Canale di pagamento

Livello: intermedio

Argomento: tecnologia

In Bitcoin, un Payment Channel di solito si riferisce a una tecnica basata su smart contract che consente agli utenti di effettuare più transazioni Bitcoin mentre regolano solo una transazione sulla rete Bitcoin, risparmiando così su commissioni e tempi di transazione. La rete Lightning sfrutta i Payment Channel.

PBKDF2

Acronimo di: Password-Based Key Derivation Function 2

Livello: avanzato

Argomento: tecnologia

PBKDF2 (funzione di derivazione della chiave basata su password 2) è la funzione utilizzata per la conversione della frase mnemonica in seed, come definito da BIP 39. E' una semplice funzione di derivazione della chiave crittografica, resistente ai dictionary attack e ai rainbow table attack.

Peg

Ancorata

Livello: intermedio

Argomento: finanza

Il termine "peg" (o ancoramento) o "pegged," che viene italianizzato come "peggato," nel contesto delle criptovalute, viene utilizzato per indicare una strategia che permette di stabilire un rapporto fisso tra due asset, spesso di categorie completamente diverse. Questo approccio viene utilizzato per vari scopi, tra cui la creazione di stablecoin ancorate alle valute fiat tradizionali o per collegare catene (chains) blockchain differenti.

Stablecoin e Ancoraggio alle Valute Fiat Uno degli utilizzi più comuni del concetto di "peg" è nell'ambito delle stablecoin. Le stablecoin sono criptovalute progettate per mantenere un valore stabile, evitando le ampie fluttuazioni di prezzo tipiche di altre criptovalute.
Per raggiungere questo obiettivo, molte stablecoin sono ancorate a valute fiat come il dollaro statunitense (USD), l'euro (EUR) o altre valute nazionali.

Una stablecoin come USDT è ancorata o peggata al dollaro, il che significa che 1 USDT dovrebbe avere un valore di 1 dollaro. Un asset è ancorato quando il suo valore è direttamente legato al valore di un altro asset sottostante. Per mantenere questo rapporto fisso di 1 a 1, le stablecoin utilizzano diverse strategie.

La modalità più semplice consiste nell'emettere la criptovaluta avendo una riserva equivalente dell'asset al quale sono ancorate. Questa riserva è definita

come “Collateral” (o garanzia), e il processo è noto come “Collateralization” (o collaterizzazione). Tuttavia, non sempre esiste questa riserva, e in generale, l’ancoraggio viene effettuato attraverso la contrazione o la diluizione dell’offerta totale dei token della stablecoin. Le variazioni nell’offerta di token influenzeranno il prezzo relativo di ciascun token, fino a raggiungere il valore desiderato.

Le stablecoin garantite, come USDT e DAI, vengono coniate e distrutte in base alle necessità, con i token appena coniati che ricevono un supporto collaterale sotto forma di altre risorse digitali. Le stablecoin algoritmiche mantengono il loro ancoraggio attraverso una combinazione di collateralizzazione e l’utilizzo di complessi algoritmi di contratti intelligenti che regolano l’offerta in base a vari fattori di mercato. Tuttavia, è importante notare che il crollo avvenuto a maggio 2022 della stablecoin UST (Terra USD) e dell’ecosistema Terra collegato ha evidenziato i rischi e la fragilità delle stablecoin algoritmiche.

Peg tra diverse criptovalute Il concetto di “peg” è altrettanto rilevante in relazione al collegamento di diversi tipi di coin o token.

Esiste la possibilità di trasferire asset e dati tra diversi coin o token, spesso su diverse chain per sfruttare le diverse funzionalità e applicazioni.

In questo contesto, i progetti di interoperabilità e cross-chain stanno emergendo per consentire il collegamento tra queste catene. Utilizzando il “peg,” è possibile bloccare un certo ammontare di una criptovaluta su una catena, emettere una rappresentazione equivalente su un’altra catena e viceversa. Questa rappresentazione ancorata consente il transito di valore o dati tra le catene in modo sicuro e affidabile.

Sidechain Il concetto di peg, con i termini derivati “peg-in,” e “peg-out” è fondamentale nel contesto delle sidechain, che sono catene blockchain ausiliarie collegate a una blockchain principale (spesso denominata mainchain). Questi termini si riferiscono alla capacità di trasferire asset o dati tra la mainchain e le sidechain in modo sicuro e affidabile. Ecco una spiegazione di ciascun concetto:

Peg-In: Il “peg-in” è il processo di trasferimento di asset dalla mainchain a una sidechain. Questo può essere fatto utilizzando un bridge o un altro metodo di trasferimento di asset cross-chain.

Quando un utente effettua un peg-in, gli asset vengono bloccati sulla blockchain principale e rilasciati sulla sidechain. Il peg mantiene il valore degli asset bloccati sulla blockchain principale allineato a quello degli asset rilasciati sulla sidechain.

Gli utenti possono effettuare il “peg-in” dei loro asset sulla sidechain per utilizzarli all’interno dell’ecosistema della sidechain. Questo processo coinvolge spesso la convalida delle transazioni sulla mainchain, seguita dalla creazione di asset equivalenti sulla sidechain, mantenendo il rapporto di ancoraggio prestabilito.

Peg-Out: Il “peg-out” è l’azione opposta al “peg-in.” Rappresenta il processo mediante il quale gli utenti trasferiscono asset dalla sidechain alla mainchain.

Quando gli utenti vogliono ritirare i loro asset dalla sidechain per utilizzarli sulla mainchain o in altre sidechain, effettuano un "peg-out." Questo processo coinvolge solitamente il blocco degli asset sulla sidechain e la successiva emissione di asset corrispondenti sulla mainchain.

Il concetto di peg, peg-in e peg-out è fondamentale per garantire l'interoperabilità tra la mainchain e le sidechain. Permette agli utenti di utilizzare asset sulla sidechain mentre mantengono la fiducia nella parità di valore tra le diverse catene. Questi meccanismi sono particolarmente importanti in contesti in cui si desidera sfruttare le funzionalità specifiche di una sidechain senza dover trasferire gli asset in modo permanente.

Ecco alcuni esempi di sidechain che utilizzano peg, peg-in e peg-out:

- **Lightning Network**: La Lightning Network è una sidechain per Bitcoin che utilizza un peg fiat per mantenere il valore dei suoi asset allineato al valore del Bitcoin.
- **RSK**: RSK è una sidechain per Bitcoin che utilizza un peg algoritmico per mantenere il valore dei suoi asset allineato al valore del Bitcoin.

penalty transaction

Livello: avanzato

Argomento: tecnologia

Una Penalty transaction, chiamata anche Justice Transaction, è un meccanismo per scoraggiare i tentativi di frode nella gestione dei canali Lightning, consentendo a una parte di un canale di recuperare i fondi rubati durante la chiusura disonesta di un canale Lightning.

Per inviare un pagamento sul canale Lightning, il mittente firma una transazione Bitcoin chiamata commitment transaction che riequilibra il canale. Questa nuova transazione viene inviata al destinatario, ma non viene trasmessa alla blockchain Bitcoin. I futuri pagamenti Lightning creeranno ulteriori commitment transaction e renderanno questa transazione obsoleta. Tuttavia, la transazione originale è ancora una transazione Bitcoin valida e può quindi essere trasmessa alla blockchain. In questo modo si chiude il canale Lightning e si annullano tutte le transazioni Lightning successive a quella originale. Ciò consente alle parti di rubare o fare un double spenging sulla rete Lightning.

Per risolvere questo problema, le commitment transaction sono impostate in modo tale che, anche dopo che una vecchia commitment transaction è stata confermata sulla blockchain, se qualcuno è in grado di produrre una commitment transaction più recente e valida dallo stesso canale, questa transazione può reclamare i fondi rubati e inoltre reclamare tutti i fondi dal lato del canale del ladro.

Il time-lock che impedisce per un tempo specificato a chi l'ha trasmessa di spendere i relativi output della transazione per un determinato tempo, consente

all'altro partner, nel caso la transazione sia obsoleta, di avere tempo per pubblicare la Penalty transaction utilizzando il secret di revoca, che gli permette di punire il comportamento scorretto rivendicando tutti i fondi del canale per sé: la transazione di force close viene revocata (Revoked Lightning Force Close) con penalità (Force closed with penalty).

Permissionless blockchain

Livello: intermedio

Argomento: tecnologia

Una blockchain permissionless (a volte indicata come pubblica) non ha restrizioni.
Chiunque disponga di una connessione Internet può accedere e non è necessaria un'autorizzazione per partecipare alla rete, per inviare transazioni ed effettuare funzioni di miner.

Se vogliamo creare un sistema senza permessi in cui chiunque possa partecipare senza chiedere, allora deve anche essere resistente agli attori disonesti.

Sono le blockchain più conosciute. Questo garantisce un più alto livello di decentralizzazione, ma per funzionare correttamente ha bisogno di una criptovaluta in modo che gli attacchi spam possano essere evitati. Bitcoin ed Ethereum sono esempi di queste blockchain.

Pickhardt Payments

Livello: avanzato

Argomento: tecnologia

I "Pickhardt Payments" sono un nuovo modo di inviare pagamenti sulla Lightning Network che sono più affidabili, convenienti e veloci rispetto ai metodi tradizionali. Questi pagamenti utilizzano un approccio intelligente per scegliere i canali di pagamento con la maggiore quantità di denaro disponibile, garantendo così che i pagamenti siano più sicuri. Inoltre, i Pickhardt Payments riducono i costi delle commissioni e consentono di instradare i pagamenti più rapidamente.

I Pickhardt Payments sono stati sviluppati da Rene Pickhardt, un ricercatore indipendente che si concentra sul miglioramento della Lightning Network. Il suo lavoro è stato ben accolto dalla comunità e i Pickhardt Payments sono ora implementati in diverse wallet e applicazioni Lightning.

A causa della modalità di progettazione dell'interconnessione dei canali Lightning Network, non viene garantito che i pagamenti inviati attraverso Lightning Network abbiano successo e quindi devono essere prese decisioni su come il wallet o il nodo dovrebbe prioritizzare il flusso di pagamento.
Un esempio è prioritizzare il percorso con le [fee(fee.html)] di routing più basse,

che è la modalità più popolare; si cerca di scegliere un percorso nella rete che comporti costi di commissioni, fee, minimizzata per il mittente.

Pickhardt Payments sono il metodo di consegna di satoshi da un nodo Lightning network a un altro utilizzando la consegna di pagamento probabilistica in un ciclo di pagamento basato su round che aggiorna la nostra conoscenza della liquidità remota nella Uncertainty Network e genera flussi di pagamento ottimizzati sull'affidabilità e convenienti in ogni round risolvendo un problema di flusso del costo minimo a pezzi linearizzato con una funzione del costo separabile.

Attualmente le due principali caratteristiche della funzione del costo sono:

- **linearized_uncertainty_unit_cost** il costo unitario di incertezza linearizzato (effettivamente proporzionale a 1/capacità del canale)
- **linearized_routing_unit_cost** e il costo unitario di routing linearizzato (effettivamente solo il ppm).

I "Pickhardt Payments" sono un metodo per inviare pagamenti sulla Lightning Network che sono più affidabili e economici rispetto ai metodi tradizionali. Funzionano utilizzando un modello probabilistico per stimare la quantità di liquidità presente in ciascun canale della rete. Il pagamento viene quindi inviato attraverso i canali con maggiore liquidità, ottimizzando l'affidabilità piuttosto che la velocità.

Ecco alcuni dei vantaggi dei Pickhardt Payments:

- Sono più affidabili rispetto ai metodi tradizionali di invio di pagamenti sulla Lightning Network. Ciò avviene perché tengono conto dell'incertezza della liquidità presente in ogni canale.
- Sono più economici rispetto ai metodi tradizionali di invio di pagamenti sulla Lightning Network. Questo perché utilizzano solo i canali con maggiore liquidità, il che significa che le commissioni sono più basse. Sono più veloci rispetto ai metodi tradizionali di invio di pagamenti sulla Lightning Network. Questo perché utilizzano solo i canali con maggiore liquidità, il che significa che i pagamenti possono essere instradati più velocemente.
- Complessivamente, i Pickhardt Payments rappresentano un miglioramento significativo rispetto ai metodi tradizionali di invio di pagamenti sulla Lightning Network. Sono più affidabili, più economici e più veloci, rendendoli il metodo preferito per inviare pagamenti sulla Lightning Network.

Ecco alcuni dettagli aggiuntivi sui Pickhardt Payments:

- Si basano sul concetto di flussi a costo minimo. Questo è un problema ben studiato nella ricerca operativa ed è stato dimostrato essere un modo efficace per trovare il percorso più efficiente per instradare un pagamento attraverso una rete.
- Sono implementati in un algoritmo basato su round. Ciò significa che il pagamento viene inviato in una serie di round e il percorso viene aggiornato dopo ogni round in base alle informazioni ottenute dal round precedente.

- Sono stati dimostrati efficaci nella pratica. In uno studio condotto da Rene Pickhardt, è stato dimostrato che i Pickhardt Payments sono stati in grado di consegnare in modo affidabile pagamenti fino al 99% del saldo locale totale del mittente.

I Pickhardt Payments rappresentano uno sviluppo promettente per la Lightning Network. Hanno il potenziale per rendere la Lightning Network più affidabile, economica e veloce, rendendola un'opzione più interessante per gli utenti.

PoA

Acronimo di: Proof-of-Authority

Livello: avanzato

Argomento: tecnologia

Un meccanismo di consenso su una blockchain che permette transazioni relativamente veloci usando la reputazione dell'identità come incentivo. Con PoA, gli individui devono guadagnarsi il diritto di diventare validatori, e quindi c'è un incentivo a mantenere la posizione che hanno acquisito. Associando una reputazione all'identità, i validatori sono incentivati a sostenere il processo di transazione, in quanto non desiderano che le loro identità siano associate a una reputazione negativa.

PoB

Acronimo di: Proof-of-Burn

Livello: avanzato

Argomento: tecnologia

Un meccanismo di consenso blockchain che mira a riavviare una blockchain in un'altra con maggiore efficienza energetica, verificando che sia stato sostenuto un costo, "bruciando" una certa quantità di moneta (inviandola a un indirizzo non modificabile e verificabile). L'idea è che i minatori debbano mostrare la prova del "burn" di alcune monete. Questo è costoso dal punto di vista individuale, proprio come la PoW (Proof-of.Work); ma non consuma risorse all'infuori della criptovaluta sottostante bruciata.

PoC

Acronimo di: Proof-of-Coverage

Livello: avanzato

Argomento: tecnologia

PoC cerca di verificare, su base continuativa, che i nodi rappresentino onestamente la loro posizione e la copertura che stanno dichiarando

pocket universe

Livello: avanzato

Argomento: tecnologia

Un pocket universe, letteralmente *universo tascabile*, è un modo per conservare collettivamente gli asset Taro e utilizzare il protocollo senza rinunciare alla proprietà degli asset.

Questo pocket universe è una singola parte (o federazione) che mantiene un commitment Taro che include beni che non può spostare unilateralmente. Un pocket universe controlla la chiave Taproot di un UTXO, ma non le chiavi degli asset Taro (eventualmente multipli) detenuti in quell'UTXO.

I possessori di asset possono usare il pocket universe per raggruppare le loro transazioni in modo efficiente.

PoD

Acronimo di: Proof-of-Developer

Livello: avanzato

Argomento: tecnologia

È un processo che cerca di connettere un progetto blockchain con i suoi reali sviluppatori. Il processo impedisce ai truffatori di rilevare un progetto, in particolare il finanziamento, senza consegnare il prodotto finale agli investitori. La PoD è comune con i progetti basati sulla criptovaluta. La PoD è stata lanciata in un momento in cui le ICO stavano prendendo piede. Alcuni emittenti di ICO cercavano solo di frodare investitori ignari. PoD consente agli investitori di guardare oltre i valori del ROI e vedere se un progetto ICO ha, in effetti, sviluppatori vivi e reali.

PoET

Acronimo di: Proof of Elapsed Time

Prova del tempo trascorso

Livello: avanzato

Argomento: tecnologia

è un algoritmo di consenso che funziona nel seguente modo:

- Ogni partecipante della rete blockchain deve attendere un periodo di tempo casuale;
- Il primo partecipante che termina l'attesa diventa leader per il nuovo blocco.

Affinché questo funzioni è necessario verificare che i partecipanti attendano effettivamente un lasso di tempo in modo casuale e che questo sia generato in un range uguale per tutti.

Poisson process

processo di Poisson

Livello: avanzato

Argomento: tecnologia

I miner Bitcoin creano blocchi tramite la Proof of Work.
La difficoltà viene regolata regolarmente in modo da mirare a un intervallo di blocco medio di 10 minuti, ma non tutti gli intervalli di blocco sono esattamente di 10 minuti.

La distribuzione dei blocchi nel tempo segue un processo statistico noto come **processo di Poisson**, secondo il quale eventi casuali si verificano con la stessa probabilità in ogni intervallo di tempo.

Un processo di Poisson, dal nome del matematico francese Siméon-Denis Poisson, è un processo stocastico che simula il manifestarsi di eventi che siano indipendenti l'uno dall'altro e che accadano continuamente nel tempo.

Nel whitepaper Bitcoin, Satoshi Nakamoto cita Poisson:

supponendo che i nodi onesti abbiano usato il tempo medio necessario per ciascun blocco, il potenziale progresso dell'attacco sarà una distribuzione di Poisson con valore atteso
Per calcolare la probabilità che un attacco possa ancora raggiungere la prova del risultato attuale, si moltiplica la densità di Poisson per ciascun tipo di progresso che potrebbe aver fatto per la probabilità che possa raggiungere la catena partendo da esso.

PoL

Acronimo di: Proof of Liabilities

Livello: avanzato

Argomento: legale

PoL o Proof of Liabilities, spesso usato insieme a PoR Proof of Reserves è la prova che che cerca di garantire che un depositario, ad esempio un CEX, non sia debitore più di un determinato importo di determinati asset.

Ad esempio, se uno Exchange può dimostrare di avere riserve di 20 mila Bitcoin e che deve ai suoi clienti non più di 19.500 Bitcoin, allora ha dimostrato che le sue partecipazioni in Bitcoin sono solvibili.

Questa prova può essere una primitiva crittografica una volta utilizzata solo per dimostrare la solvibilità finanziaria, ma è applicabile anche a domini al di fuori della finanza, comprese donazioni trasparenti e private.

Ponzi

Livello: base

Argomento: legale

gli schemi Ponzi sono, fondamentalmente, attività di investimento fraudolente che funzionano ripagando gli investitori che sono entrati prima nel sistema con denaro raccolto da nuovi investitori. Questi schemi fraudolenti vengono solitamente presentati come servizi di gestione degli investimenti, in cui i partecipanti ritengono che il rendimento che otterranno sia il risultato di un investimento legittimo. Gli impostori spesso attirano gli investitori promettendo profitti rapidi e/o elevati, ma in realtà il truffatore sta fondamentalmente derubando un investitore per pagare l'altro. Il problema con un tale schema è che quando diminuisce la crescita degli investitori, gli ultimi che arrivano non verranno mai pagati. Lo schema Ponzi prende il nome da Charles Ponzi, un truffatore italiano che si trasferì in Nord America e divenne famoso per il suo sistema fraudolento con il quale negli anni '20 riuscì a frodare centinaia di vittime per oltre un anno.

PoR

Acronimo di: Proof of Reserves

Livello: avanzato

Argomento: legale

La Proof of Reserves (PoR) è un audit che cerca di garantire che un depositario, ad esempio un CEX, detenga gli asset che i suoi clienti hanno nei loro conti presso il depositario.

Proof of Reserves è l'idea che le società di custodia che detengono criptovalute creino attestazioni rivolte al pubblico in merito alle loro riserve, abbinate a una prova dei saldi degli utenti.

L'audit per essere credibile dovrebbe essere condotto da una terza parte affidabile, un revisore indipendente, ma alcuni depositari effettuano la PoR in modalità self-assessment, ovvero le hanno fatto per conto loro con la pretesa di essere credibili.

L'idea è dimostrare al pubblico in generale, e in particolare ai tuoi depositanti, che le criptovalute detenute in deposito corrisponde ai saldi degli utenti. Naturalmente, in pratica, non è così semplice, la PoR può dare agli utenti un falso senso di sicurezza. Dimostrare di controllare alcuni fondi on-chain può essere semplice, ma questo potrebbe essere sempre fatto prendendo in prestito quei fondi a breve termine. Questo è il motivo per cui le attestazioni point-in-time

significano relativamente poco. Inoltre, o i CEX possono avere passività nascoste o i creditori che rivendicano privilegi rispetto ai depositanti.

Pertanto, una piattaforma potrebbe utilizzare la PoR per apparire come un soggetto autoregolamentato e trasparente senza rivelare il suo vero rischio di solvibilità.

A volte la PoR viene presentata insieme alla PoL Proof of Liabilities.

Tecnicamente questo audit può essere fatto acquisendo un'istantanea anonima di tutti i saldi detenuti e aggregarli in un Merkle Tree, una struttura di dati rispettosa della privacy che incapsula tutti i saldi dei clienti.

Da questa, l'auditor ricava una Merkle root: un'impronta digitale crittografica che identifica in modo univoco la combinazione di questi saldi al momento della creazione dello snapshot.

L'auditor raccoglie quindi le firme digitali prodotte dal depositario, che dimostrano la proprietà degli indirizzi on-chain con saldi verificabili pubblicamente. Infine, l'auditor confronta e verifica che questi saldi superino o corrispondano ai saldi dei clienti rappresentati nel Merkle Tree e quindi che le attività del cliente siano detenute con riserva integrale.

Il Merkle Tree consente di verificare l'accuratezza di tutti i saldi incrociando solo alcuni saldi anonimi con quelli verificati. Ad esempio, qualsiasi utente può verificare se il suo vero saldo del conto è stato incluso nel Merkle Tree.

Una serie di verifiche di questo tipo può essere utilizzata per dimostrare l'accuratezza dell'intero albero, senza esaminare ogni singolo elemento.

Sebbene la soluzione incorpori elementi della tecnologia blockchain, richiede comunque fiducia nei revisori dei conti di terze parti e nelle pratiche contabili che valutano le attività off-chain, e ogni cliente dovrebbe poter verificare in modo indipendente che il proprio saldo sia stato incluso nell'audit Proof of Reserves confrontando dati selezionati con la Merkle root. Qualsiasi modifica apportata al resto dei dati, per quanto piccola, influirà sulla root hash; rendendo evidente la manomissione.

Dimostrare le passività è complicato e generalmente richiede che un revisore si impegni in una valutazione completa. Ad esempio, i CEX possono omettere determinate responsabilità per "imbrogliare" un'attestazione PoR.

Portfolio

Livello: intermedio

Argomento: tecnologia

Una raccolta di criptovalute o asset finanziari detenuti da una società di investimento/ hedge fund/ istituto finanziario. Spesso è anche usato come termine che indica semplicemente tutte le criptovalute possedute da un individuo.

PoS

Acronimo di: Proof-of-Stake

Livello: intermedio

Argomento: tecnologia

Il Proof-of-stake è un meccanismo di consenso nel quale i validatori di blocco vengono selezionati in base al numero di coin che stanno vincolando.

"Proof of Stake" - letteralmente la "prova della posta in gioco (inteso anche come stake-possesso)" anche se non c'è nessuna prova, non c'è nessuna posta in gioco e non è lontanamente paragonabile alla proof-of-work Bitcoin nonostante l'assonanza del termine.

La proof-of-work ha risolto il problema dello stabilire la sequenza del tempo in un sistema decentralizzato, il problema della selezione casuale, il problema dell'emissione equa e il problema dell'inesigibilità dei costi nel regno digitale. Incorpora direttamente la verità oggettiva in un blocco di dati, ed è per questo che non ha bisogno di qualcuno di cui trasferire la nostra fiducia e affidabile. Le informazioni "parlano da sole", per citare Satoshi.

La proof-of-stake, invece, non ha una verità oggettiva, non ha un tempo oggettivo, non ha una selezione casuale, non ha un'emissione equa, non ha costi esterni, non ha costi operativi e si centralizza nel tempo. È la macchina del moto perpetuo dei meccanismi di consenso, il che significa che non è affatto un meccanismo di consenso. È fondamentalmente corrotto perché si basa, in tutto e per tutto, sulla fiducia in una terza parte.

La proof-of-stake dovrebbe chiamarsi "fidati di me, credici", perché chiamandola proof-of-stake, si potrebbe pensare che sia paragonabile alla proof-of-work. Sbagliato. La proof-of-stake è una finzione perché porta inevitabilmente a tutti i problemi di cui soffre il sistema monetario basato sulla valuta a corso forzoso, o fiat.

Il termine "staking" si riferisce all'atto dei validatori che stanno impegnano i loro fondi nel sistema. Quindi i validatori possono partecipare al processo di produzione di nuovi blocchi solo se bloccano i loro coin. I fondi bloccati fungeranno quindi da garanzia, il che significa che i validatori dannosi molto probabilmente perderanno i loro importi e verranno espulsi dalla rete. Mentre i validatori onesti verranno premiati man mano che vengono prodotti (coniati) nuovi blocchi.

PoSpace

Acronimo di: Proof-of-Space

Livello: avanzato

Argomento: tecnologia

È un meccanismo di consenso in cui si utilizza lo spazio disco o di memoria per l'algoritmo di consenso

PoST

Acronimo di: Proof-of-Spacetime

Livello: avanzato

Argomento: tecnologia

è un tipo di algoritmo di consenso ottenuto dimostrando il proprio interesse legittimo in un servizio allocando una quantità non banale di memoria o spazio su disco per risolvere una sfida presentata dal fornitore di servizi.

PoT

Acronimo di: Proof-of-Trust

Livello: avanzato

Argomento: tecnologia

è un meccanismo di consenso in cui gli utenti "mettono in gioco" la fiducia che hanno guadagnato in una rete al fine di verificare le transazioni di criptovaluta. In un sistema proof of trust, gli utenti guadagneranno un valore virtuale chiamato "trust" ogni volta che acquisiranno un ruolo nell'ecosistema. Un nodo altamente affidabile sarà in grado di verificare le transazioni di valore uguale o inferiore alla fiducia accumulata da questo utente. Un nodo con scarsa attendibilità sarà in grado di verificare solo transazioni inferiori al loro valore equivalente. Il modo in cui la fiducia viene convertita in valore e viceversa dipende da ciascuna implementazione

PoW

Acronimo di: Proof-of-Work

Livello: base

Argomento: tecnologia

La PoW, Proof of Work o prova di lavoro, è il modo introdotto da Bitcoin, con il quale i miner mettono in sicurezza la creazione di nuovi blocchi e il loro inserimento all'interno della blockchain.
La PoW è una forma di prova crittografica con la quale il miner dimostra agli altri partecipanti alla rete di aver effettuato un notevole sforzo nell'effettuare i calcoli necessari per poter inserire il nuovo blocco in blockchain, e questo rende proibitivo modificare i blocchi inseriti in blockchain dovendo rifare tutti i calcoli.

Per compensare l'aumento della velocità dell'hardware e la partecipazione dei nodi nel tempo, la difficoltà della PoW è determinata da una media mobile

impostata in modo da avere circa un nuovo blocco in media ogni 10 minuti.
Se i blocchi vengono generati troppo velocemente, la difficoltà aumenta. La difficoltà nei primi anni di vita dei bitcoin consentiva di fare mining utilizzando la CPU, poi si è passati alle GPU e infine agli Asic.

PPLNS

Acronimo di: Pay-Per-Last-N-Shares

Livello: avanzato

Argomento: tecnologia

PPLNS è un tipo di pagamento dei miner che partecipano ad una mining pool, tramite il quale i profitti sono assegnati in base al numero di share con i quali i miner contribuiscono.

Questo tipo di metodo di allocazione è strettamente legato al blocco estratto. Se il mining pool estrae più blocchi in un giorno, i miner avranno un profitto elevato; se il mining pool non è in grado di estrarre un blocco durante l'intera giornata, il profitto del miner durante l'intera giornata è pari a zero.

In particolare, nel breve termine, il modello PPLNS è altamente correlato alla fortuna di un pool. Se il fattore fortuna di un particolare mining pool diminuisce nel breve termine, anche il reddito del miner diminuirà di conseguenza (è possibile anche il caso opposto in cui il mining pool sia fortunato nel breve termine). Tuttavia, nel lungo periodo, il fattore fortuna tende a raggiungere la media.

Pertanto, questo modello è ideale per fissare ordini su un grande pool che ha un'alta probabilità di trovare un blocco entro il limite di tempo dell'ordine. Oppure un ordine standard che prevede la connessione dei miner per un periodo di tempo più lungo.

ppm

Acronimo di: parts per million

parti per milione

Livello: avanzato

Argomento: tecnologia

ppm, parti per milione è l'unità di misura generalmente utilizzata per la fee_rate dei canali di Lightning Network.

Quando si utilizza il termine "PPM fee" ci si riferisce al valore in ppm del fee_rate.

È una fee che viene impostata da chi gestisce il canale Lightning, con un valore percentuale dell'importo del pagamento che viene inoltrato attraverso il canale, con lo scopo di compensare il capitale che viene impegnato nei canali Lightning.

La fee_rate è una fee proporzionale applicata in base al valore di ogni HTLC inoltrata.

In genere è espressa in ppm, anche se il comando `lncli updatechanpolicy` utilizza cifre decimali.

Il valore di default è 1 mSAT, pari allo 0,0001% della transazione. Un valore impostato generalmente può essere compreso tra 10 e 1000, a seconda della popolarità del canale per l'instradamento delle transazioni.

Per fare un esempio pratico: se qualcuno invia 1M di SAT su un canale con una tariffa di 100 PPM, il gestore del canale incasserà 100 SAT.

Naturalmente, più alte sono le fee, più si guadagna, ma questo rende anche meno probabile che il nodo mittente scelga un canale per instradare il pagamento se ha fee più alte. In genere i nodi sono configurati per cercare i canali con le fee più basse.

Un metodo per impostare è quello di sperimentare impostando fee molto basse per stabilire una linea di base per il numero di transazioni che si instradano normalmente, e poi aumentarle gradualmente verificando con quale importo il volume delle transazioni inizia a diminuire. Inoltre, è bene tenere presente che le fee possono variare nel tempo. Altri nodi potrebbero soddisfare un determinato percorso o potrebbero abbandonarlo, dando l'opportunità di impostare fee più alte.

Si può visualizzare attraverso il comando `lncli feereport` che restituisce per comodità sia il valore decimale (fee_rate) sia l'importo per milione (fee_per_mil).

PPS

Acronimo di: Pay-Per-Share

Livello: avanzato

Argomento: tecnologia

PPS è un tipo di pagamento dei miner che partecipano ad una mining pool, che offre un pagamento istantaneo e forfettario per ogni share, o quota, risolta.

Con share si intende le quantità discrete di lavoro valido che hanno contribuito al pool da ciascun miner o mining farm. Il valore di ciascuna share è determinato dall'attuale difficoltà di rete del criptoasset e dal numero di contributi di share totali da parte dei miner o mining farm.

Con questo metodo di pagamento, un miner riceve un tasso di pagamento standard per ogni share completata. Ogni share vale una certa quantità di criptovaluta estraibile.

Dopo aver dedotto le commissioni del pool di mining, i miner ricevono un reddito fisso ogni giorno. Pertanto, con la modalità PPS, i rendimenti sono relativamente stabili. I miner sono esposti al rischio. Potrebbero non ricevere le transaction fee.

Sebbene i pagamenti siano distribuiti indipendentemente dal fatto che un pool trovi con successo un blocco, probabilisticamente, i blocchi verranno trovati con successo in modo statisticamente prevedibile dal pool, che dipende dalla quantità totale dalla hashing power (shares) apportata dai miner e dalle mining farm. Questa è una strategia che fornisce pagamenti regolari, elimina il fattore del mining dovuto alla fortuna e spesso fornisce ai miner pagamenti immediati.

PPS+ è un misto della modalità PPS con quella PPLNS. La ricompensa del blocco viene regolata secondo il modello PPS. E la fee charge/transaction del servizio di mining è regolata secondo la modalità PPLNS.

Paga i premi fissi del blocco con lo schema di pagamento PPS e distribuisce le fee delle transazioni che il pool ha estratto con lo schema di pagamento PPLNS (Pay Per Last N Share). Con lo schema di pagamento PPS, i miner possono ricevere transaction fee oltre ai ricavi calcolati dallo schema di pagamento PPS.

In altre parole, in questa modalità, il miner può ottenere in aggiunta il reddito di una parte della transaction fee in base al metodo di pagamento PPLNS, che è uno dei principali svantaggi del modello PPS.

Pre-mine

Pre-minato

Livello: intermedio

Argomento: tecnologia

Con pre-mine o pre-mined, ma anche instamined o fast mined con diverse sfumature di significato, in italiano traducibile con pre-minato, si intende quando una parte o tutta l'offerta iniziale di una criptovaluta viene generata durante o prima che sia resa disponibile al pubblico, invece che essere generata successivamente alla sua pubblicazione dilazionando l'emissione nel tempo attraverso il mining o l'inflazione.

Alcuni progetti hanno distribuzioni di token o coin inique perché sono stati premined dai fondatori del progetto, acquisendo di fatto una posizione di vantaggio fin dal lancio iniziale del progetto.

Bitcoin non è stato preminato, questo è dimostrabile ad esempio dal Genesis Block che contiene il titolo di un articolo del giornale The Times della stessa data del blocco 3 gennaio 2009, e questo perché non si possa minare un blocco

senza conoscerne il suo contenuto, e i blocchi successivi non possono essere minati prima di questo poiché ogni blocco è collegato nella blockchain al blocco precedente tramite il suo hash. Ethereum è un esempio di criptovaluta che ha visto un gran numero di monete pre-miniate prima della sua ICO.

Il pre-mining è una pratica simile alla vendita di una quota di un'azienda ai dipendenti prima che l'impresa diventi pubblica attraverso un'offerta pubblica iniziale (IPO).

Nel caso di una valuta digitale, le monete create in precedenza - e messe da parte prima del lancio della valuta - creeranno valore per i loro possessori dopo essere diventate negoziabili. Spesso questi primi coin o token andranno agli investitori dell'ICO, agli sviluppatori e ai membri del team che hanno contribuito alla nascita della valuta.

Questa pratica del pre-mining viene da alcuni considerata deprecabile, altri la ritengono una modalità adeguata al finanziamento dei progetti, per ricompensare gli sviluppatori e i dipendenti che partecipano alla progettazione e alla modellazione del progetto e che ciò incentivi la loro partecipazione. Tuttavia, il pre-mining rimane una pratica oscura per molti, in quanto genera sfiducia negli utenti. Alcuni sviluppatori di nuovi progetti effettuano il pre-mining e accantonano un gran numero di monete prima dell'ICO, senza comunicare questa informazione al pubblico e poi, quando la criptovaluta viene lanciata e i prezzi si gonfiano a causa della mancanza di monete disponibili, possono rilasciare le loro monete pre-miniate sul mercato, causando un forte calo del loro prezzo e danneggiando gli outsider.

Pre-sale

Livello: intermedio

Argomento: finanza

Una vendita che avviene prima che un ICO sia messo a disposizione del pubblico per il finanziamento.

preimage

Livello: avanzato

Argomento: tecnologia

Il preimage è l'hash della preimage, chiamato anche payment secret o payment preimage. I pagamenti su Lightning Network vengono effettuati su questo hash della preimage, che deve essere rivelato dal beneficiario per richiedere il pagamento. Se il beneficiario non rivela la preimage, il pagamento può essere reclamato dal mittente dopo un periodo di timeout. Quando su Lightning Network si invia un pagamento lungo diversi canali ogni passaggio effettua un pagamento

alla stessa preimage, e in questo modo viene assicurato che il pagamento possa essere reclamato nella sua interezza o che fallisca: atomicità.

Lightning Network gestisce questa cosa tramite un HTLC, Hash Time-lock Contract, una transazione bitcoin che può essere riscattata producendo la preimage (Hash) o aspettando un periodo di tempo predefinito (Time). L'hash diventa la condizione di pagamento nella transazione bitcoin e, una volta rivelato il segreto, tutti i partecipanti possono riscattare i pagamenti in arrivo. Gli HTLC offrono atomicità, operazioni trustless, e sicurezza multihop (il routing tra i canali).

Private Blockchain

Blockchain Privata

Livello: intermedio

Argomento: tecnologia

E' una blockchain all'interno della quale per partecipare bisogna essere autorizzati. Se si vuole interagire in essa o diventarne un miner o un validatore è necessario essere invitato dall'autorità centrale che la governa. Questo tipo di blockchain viene di solito utilizzato da società di marketing o per fini educativi.

Private Key

Chiave privata

Livello: base

Argomento: tecnologia

Una chiave privata Bitcoin è codice che rappresenta l'accesso al controllo di un indirizzo Bitcoin. In altre parole, la chiave privata è l'elemento che ti permette di spendere i fondi associati all'indirizzo Bitcoin.

La chiave privata viene generalmente memorizzata nel wallet, consente di firmare le transazioni e in questo modo rappresenta le credenziali digitali dei vostri bitcoin, e per certi versi potrebbe essere considerata come una password: chiunque sia in possesso di tale chiave privata potrà gestire quei fondi sulla blockchain.

La chiave privata deve rimanere sempre segreta, perché rivelarla a terzi equivale a dare loro il controllo sui bitcoin protetti da quella chiave. Bisogna inoltre fare un backup, o salvare da qualche parte, la chiave privata affinché sia protetta da perdite accidentali, perché se viene persa non può essere recuperata e anche i fondi garantiti da essa sono persi per sempre.

Dalla chiave privata viene derivata la chiave pubblica.

La chiave privata è un numero di solito generato in modo casuale.

La chiave privata bitcoin è solo un numero. Si può scegliere la propria chiavi privata in modo casuale anche semplicemente usando solo una moneta, una

matita e un foglio: si lancia una moneta 256 volte per scegliere i valori 0 o 1 delle 256 cifre binarie di una chiave privata casuale che si possono utilizzare in un wallet bitcoin. La chiave pubblica può quindi essere generata dalla chiave privata.

Formati della chiave privata La chiave privata può essere rappresentata in diversi formati, che corrispondono tutti allo stesso numero a 256 bit. Le rappresentazioni delle chiavi private (formati di codifica) mostrano tre formati comuni utilizzati per rappresentare le chiavi private. Formati diversi vengono utilizzati in circostanze diverse. I formati esadecimali e binari non elaborati vengono utilizzati internamente nel software e raramente mostrati agli utenti. Il WIF viene utilizzato per l'importazione

Rappresentazioni delle chiavi private (formati di codifica)

Tipo	Prefisso	Descrizione
Raw	nessuno	32 byte
Hex	nessuno	64 cifre esadecimali
WIF	5	Codifica Base58Check: Base58 con prefisso 0x80 e checksum a 4 byte
WIF-compressed	K o L	Come per WIF, con l'aggiunta del suffisso 0x01 prima della codifica

Seed

Spesso la chiave privata viene confusa con il seed, che sono concetti correlati nell'ambito delle criptovalute, ma non sono la stessa cosa.

Il seed è una frase composta da diverse parole, spesso 12 o 24, che viene utilizzata come seed o seme per generare una o più chiavi private. Il seed viene utilizzato come una forma di backup e ripristino delle chiavi del wallet, in modo da poter accedere ai propri fondi in caso di perdita o danneggiamento del dispositivo sul quale è memorizzato il wallet.

La chiave privata è generata a partire dal seed utilizzando un'algoritmo deterministico che consente di generare molte chiavi private da un singolo seed. In questo modo, se si conosce il seed, è possibile generare la chiave privata associata e accedere ai propri fondi.

Chiave privata estesa

La chiave privata estesa è un formato che include informazioni extra, come i codici di derivazione dei segni, insieme alla chiave privata vera e propria. Questo formato viene utilizzato in alcuni tipi di wallet hardware e software per supportare la gestione delle più complesse gerarchie di chiavi e indirizzi.

Private sale

Vendita privata

Livello: intermedio

Argomento: finanza

la prima fase di una ICO, IEO, STO, in cui i token vengono venduti a un certo prezzo, solitamente preferenziale, a investitori specifici contattati per finanziare un progetto crittografico prima del suo lancio ufficiale. Non è una fase obbligatoria di una vendita di token.

Protocol

Protocollo

Livello: base

Argomento: tecnologia

Un protocollo è un insieme di regole o procedure che governano un sistema.
In una rete di computer, un protocollo è un programma comune eseguito da più computer sulla stessa rete.

Questi protocolli di rete regolano la trasmissione e la gestione delle informazioni, nonché l'esecuzione di programmi tra dispositivi interconnessi ma indipendenti.

Nelle reti criptovalute, il protocollo più importante è il protocollo di consenso: è il protocollo seguito da ciascun partecipante alla rete (o nodo) per creare un singolo stato condiviso della block chain.
In questo contesto, i protocolli di consenso sostituiscono un registratore o una controparte centralizzata, consentendo interazioni peer-to-peer senza doversi affidare a soggetti fiduciari.

Pruned node

Livello: avanzato

Argomento: tecnologia

Per evitare di memorizzare tutta la blockchain su disco è possibile eseguire un nodo in una modalità definita Pruned mode.
Il full node in questo caso viene definito **pruned node**.

La modalità *pruned* per un nodo Bitcoin si riferisce alla configurazione di un nodo che conserva su disco solo una parte dell'intera blockchain Bitcoin. Questo significa che il nodo non conserva una copia completa della blockchain, ma solo una copia delle parti essenziali per il suo funzionamento.

In particolare, un nodo Bitcoin in modalità pruned elimina tutte le transazioni più vecchie rispetto ad un certo punto di blocco specificato (detto "punto di pruning") dalla sua memoria. In questo modo, il nodo occupa meno spazio su disco e richiede meno risorse di elaborazione, ma può ancora verificare le transazioni più recenti e partecipare alla rete Bitcoin.
Anche se il nodo pruned conserva soltanto i blocchi più recenti, deve comunque effettuare l'IBD Initial Block Download, ovvero scaricare tutti i blocchi per effettuare le verifiche.

Da notare che la modalità *pruned* può comportare alcune limitazioni per i nodi che la utilizzano, ad esempio non saranno in grado di fornire copie complete della blockchain ad altri nodi che li richiedono.

Per abilitare la modalità pruned bisogna impostare il parametro prune=N all'avvio o in bitcoin.conf, dove N è il numero di MiB da allocare. Il valore 0 disabilita modalità prune.

Il valore minimo sopra 0 è 550, circa mezzo giga.

In relazione al tempo di caricamento necessario esiste una proposta chiamata AssumeUTXO per predisporre una modalità che consenta l'avvio di un full node senza la necessità di completare l'IBD, che ha comunque caratteristiche diverse dalla modalità *pruned*.

PSBT

Acronimo di: Partially Signed Bitcoin Transaction

Transazione Bitcoin parzialmente firmata

Livello: avanzato

Argomento: tecnologia

Una transazione PSBT, Partially Signed Bitcoin Transaction o transazione Bitcoin parzialmente firmata, è uno standard Bitcoin che facilita la portabilità delle transazioni non firmate, consentendo a più parti di firmare facilmente la stessa transazione. Questo è molto utile quando più parti desiderano aggiungere input alla stessa transazione.

È un formato di interscambio che, tra l'altro, può essere utilizzato per gestire scenari più complessi in cui sono coinvolte firme di più soggetti (es. wallet multi signature). Un formato di transazione che contiene le informazioni necessarie a un firmatario per produrre firme per la transazione e contiene le firme per un input mentre l'input non ha un set completo di firme. Il firmatario può essere offline poiché tutte le informazioni necessarie verranno fornite nella transazione.

La creazione di transazioni non firmate o parzialmente firmate da passare a più firmatari è attualmente dipendente dall'implementazione, rendendo difficile per le persone che utilizzano wallet diversi la possibilità di farlo facilmente. Uno degli obiettivi di questo sistema è creare un formato standard ed estensibile che possa essere utilizzato tra i clienti per consentire alle persone di passare la stessa transazione per firmare e combinare le proprie firme. Il formato è anche progettato per essere facilmente esteso per un uso futuro, cosa più difficile da fare con i formati di transazione esistenti. La firma delle transazioni richiede inoltre che gli utenti abbiano accesso agli UTXO spesi. Questo formato di transazione può consentire ai firmatari offline come i wallet air-gapped e i wallet hardware di essere in grado di firmare transazioni senza bisogno di accedere direttamente al set UTXO e senza il rischio di essere frodati.

PSBTv2

Livello: avanzato

Argomento: tecnologia

PSBT Version 2. Consente di aggiungere input e output a PSBT dopo la creazione. PSBT non è in grado di aggiungere nuovi input e output alla transazione. La transazione globale non firmata fissa non può essere modificata, il che impedisce l'aggiunta di ulteriori input o output. PSBT versione 2 ha lo scopo di correggere questo problema.

PTLC

Acronimo di: Point Time Locked Contracts

Livello: avanzato

Argomento: tecnologia

L'introduzione da parte di Taproot delle firme Schnorr apre la strada a un tipo di smart contract chiamato PTLC (Point Time Locked Contracts).

I PTLC funzionano allo stesso modo degli HTLC consentendo ai nodi di identificare i pagamenti, ma i PTLC sono dotati di una comoda funzione di poter randomizzare il proprio identificatore con ogni hop, rendendo così impossibile per i nodi correlare il traffico dei nodi di invio e ricezione.

I Point Time Locked Contracts (PTLC) sono pagamenti condizionati che possono sostituire l'uso degli HTLC nei canali di pagamento Lightning Network,

nei Coinswap sulla stessa chain, in alcuni atomic swap cross-chain e in altri protocolli di smart contract. Rispetto agli HTLC, possono essere più privati e utilizzare meno spazio per i blocchi.

I PTLC si differenziano dagli HTLC per il metodo di blocco e sblocco principale:

- HTLC hash lock: sono bloccati utilizzando un hash digest e sbloccati fornendo la corrispondente preimage. La funzione di hash più comunemente utilizzata è SHA256, che produce un digest a 256 bit (32 byte) generato da una preimage a 32 byte. Quando viene utilizzato per proteggere più pagamenti (ad esempio, un pagamento Lightning Network instradato o un atomic swap), tutti i pagamenti utilizzano la stessa preimage e lo stesso hash lock. Questo crea un collegamento tra i pagamenti se vengono pubblicati on-chain o se vengono instradati off-chain attraverso nodi di sorveglianza.
- PTLC point lock: sono bloccati utilizzando una chiave pubblica (un punto sulla curva ellittica di Bitcoin) e sbloccate fornendo una firma corrispondente da un signature adaptor soddisfatto. Per la costruzione della firma Schnorr proposta, la chiave sarebbe di 32 byte e la firma di 64 byte. Tuttavia, utilizzando ECDSA multiparty o l'aggregazione e la firma delle chiavi di Schnorr, le chiavi e la firma possono essere combinate con altre chiavi e altre firme necessarie per autorizzare qualsiasi spesa, consentendo ai point lock di utilizzare zero byte di spazio di blocco distinto. Ogni point lock può utilizzare chiavi e firme diverse, quindi non c'è nulla nel point lock che correli i diversi pagamenti sia on-chain che quando vengono instradati off-chain attraverso nodi di sorveglianza.

L'implementazione dei PTLC in Bitcoin richiede la creazione di signature adaptor che sono più facili da combinare da quando le firme di Schnorr sono state implementate in Bitcoin. Per questo motivo, lo sviluppo di PTLC in Bitcoin è stato per lo più un argomento di discussione piuttosto che un lavoro attivo. L'indisponibilità delle firme schnorr nelle criptovalute alternative può anche impedire l'uso delle PTLC in alcuni contratti cross-chain, sebbene sia ancora tecnicamente possibile utilizzare le PTLC con le sole chiavi elettroniche e firme ECDSA.

Public blockchain

Blockchain pubblica

Livello: base

Argomento: tecnologia

vedi Permissionless blockchain

Public Key

Chiave pubblica

Livello: base

Argomento: tecnologia

Una chiave pubblica è la chiave che viene data ad altre persone come destinazione per ricevere i pagamenti, potremmo considerarla l'equivalente di un indirizzo fisico o di una e-mail.

È l'informazione che occorre fornire per farsi inviare criptovalute. In un tipico sistema a chiave pubblica, un utente genera una chiave privata e una chiave pubblica, mantiene la chiave privata segreta e può fornire la chiave pubblica a tutti.

Tali destinatari possono crittografare le informazioni con la chiave pubblica, e queste possono essere decrittate con la chiave privata ma non possono essere decrittate con la stessa chiave pubblica a causa dell'asimmetria della coppia di chiavi.

Una chiave privata può essere convertita in una chiave pubblica, ma una chiave pubblica non può essere riconvertita in una chiave privata perché la matematica funziona solo in un modo.

La chiave pubblica viene calcolata dalla chiave privata utilizzando la moltiplicazione della curva ellittica, che è irreversibile: K = k * G, dove k è la chiave privata, G è un punto costante chiamato punto generatore e K è la chiave pubblica risultante. L'operazione inversa, nota come "trovare il logaritmo discreto" - calcolare k se si conosce K - è difficile quanto provare tutti i possibili valori di k, cioè una ricerca a forza bruta.

La moltiplicazione della curva ellittica è un tipo di funzione che i crittografi chiamano funzione "unidirezionale": è facile da eseguire in una direzione (moltiplicazione) e impossibile da eseguire nella direzione inversa ("divisione", o trovare il logaritmo discreto) . Il proprietario della chiave privata può facilmente creare la chiave pubblica e quindi condividerla con il mondo sapendo che nessuno può invertire la funzione e calcolare la chiave privata dalla chiave pubblica.

Generazione di una chiave pubblica

Partendo da una chiave privata sotto forma di un numero k generato casualmente, lo moltiplichiamo per un punto predeterminato sulla curva chiamato punto generatore G per produrre un altro punto da qualche altra parte sulla curva, che è la chiave pubblica corrispondente K. Il punto generatore è specificato come parte dello standard secp256k1 ed è sempre lo stesso per tutte le chiavi in bitcoin.

Formato della chiave pubblica nelle transazioni bitcoin

Una chiave pubblica Bitcoin può essere nel formato non compressa, o nel formato compresso.

Chiave pubblica non compressa Quando una chiave pubblica è rappresentata in formato non compresso, ha la seguente struttura:

- 04: prefisso Indica che è una chiave pubblica non compressa.
- X (32 byte): La coordinata x del punto sulla curva.
- Y (32 byte): La coordinata y del punto sulla curva.

Quindi, la lunghezza totale della chiave pubblica non compressa è:
1 byte (prefisso 04) + 32 byte (x) + 32 byte (y) = 65 byte (520 bit).

Chiave pubblica compressa Per risparmiare spazio, è possibile comprimere la chiave pubblica.

Le curve ellittiche utilizzate nella crittografia per Bitcoin sono simmetriche rispetto all'asse X. Questo significa che se un punto (x, y) si trova sulla curva, allora anche il punto (x, -y) si trova sulla curva.

Conoscendo la coordinata x, esistono solo due possibili valori per y (uno positivo e uno negativo rispetto alla curva).

In questo caso, il prefisso diventa:

- 02 Se la coordinata y è pari.
- 03 Se la coordinata y è dispari.

Al quale seguono i 32 byte della coordinata x

Quindi, la chiave pubblica compressa è lunga 33 byte (264 bit) invece di 65.

La chiave pubblica viene usata nelle transazioni di tipo P2PK. Tuttavia, per le transazioni Bitcoin, generalmente si usa l'indirizzo Bitcoin, che è una derivazione dell'hash della chiave pubblica.

Indirizzo bitcoin ottenuto dalla chiave pubblica

L'indirizzo Bitcoin è derivato dalla chiave pubblica attraverso l'uso dell'hashing crittografico unidirezionale.

Puell Multiple

Livello: avanzato

Argomento: tecnologia

Il Puell Multiple, multiplo di Puell, è un modo per valutare i cicli di mercato dal punto di vista della redditività del mining / ricavi dei compulsory seller.

Prende i ricavi totali dei miner e le aggiusta in base alla loro media mobile annuale.

Calcolo = ricavi miner / media mobile semplice di 365 giorni dei ricavi miner

Il Puell Multiple si concentra sull'offerta dell'economia di Bitcoin, e in particolare sui miner di BTC e sulle loro entrate. In altre parole, esamina i cicli di mercato dal punto di vista dei profitti dei miner.

Viene calcolato dividendo il valore in USD dei Bitcoin emessi ogni giorno per la media mobile a 365 giorni del valore dell'emissione giornaliera.

Pump & Dump

Livello: base

Argomento: finanza

Questi due termini sono traducibili in "pompare" e "scaricare". Si tratta della tecnica usata da traders esperti per guadagnare sfruttando la propria disponibilità finanziaria. Viene effettuata facendo gonfiare in modo artificiale il prezzo attraverso acquisti, dichiarazioni positive false e fuorvianti, al fine di vendere l'azione acquistata a buon mercato a un prezzo più alto. Una volta che gli operatori fanno il dump, vendendo le loro azioni sopravvalutate, il prezzo scende e gli investitori si trovano ad avere criptovalute che valgono meno di quanto le hanno pagate.

QE

Acronimo di: Quantitative Easing

Allentamento quantitativo

Livello: intermedio

Argomento: politica

Il quantitative easing è l'incremento dell'offerta monetaria attuata dalle banche centrali, è un tipo di politica monetaria progettata per stimolare le economie o sostenere i prezzi, e tende ad aumentare l'inflazione. Il quantitative easing è normalmente impiegato durante i periodi di recessione.

Nel marzo 2020, la Federal Reserve nordamericana ha iniziato a condurre la sua quarta operazione di quantitative easing dalla crisi finanziaria del 2008; il 15 marzo 2020 ha annunciato circa 700 miliardi di dollari di nuovo allentamento quantitativo tramite acquisti di attività per sostenere la liquidità degli Stati Uniti in risposta alla pandemia di COVID-19. A metà estate 2020 ciò si è tradotto in ulteriori $ 2 trilioni di attività sui registri della Federal Reserve. La Banca Centrale Europea il 18 marzo 2020, per aiutare l'economia ad assorbire lo shock della crisi COVID-19, ha annunciato un Pandemic Emergency Purchase

Programme, programma di acquisto di emergenza pandemica (PEPP) da 750 miliardi di euro. L'obiettivo del pacchetto di stimolo (PEPP) era ridurre i costi di finanziamento e aumentare i prestiti nell'area dell'euro.

La strategia del quantitative easing viene implementata quando una banca centrale aggiunge denaro a un'economia, generalmente acquistando titoli e obbligazioni dal mercato. E' una forma di politica monetaria non convenzionale in cui una banca centrale acquista titoli a più lungo termine dal mercato aperto per aumentare l'offerta di moneta e incoraggiare prestiti e investimenti. Ciò si traduce in un aumento dell'offerta di moneta. Il quantitative easing crea una domanda artificiale di asset, aumentandone i prezzi. L'acquisto di strumenti di debito riduce il loro rendimento, con conseguente riduzione dei tassi di interesse. Ciò incentiva gli investimenti e l'attività economica più rischiosi. L'allentamento quantitativo alla fine si traduce in inflazione per l'economia, a causa dell'aumento dell'offerta di moneta.

L'acquisto di questi titoli aggiunge nuovo denaro all'economia e serve anche ad abbassare i tassi di interesse offrendo titoli a reddito fisso. Espande anche il bilancio della banca centrale.

QR Code

Livello: base

Argomento: tecnologia

Un'etichetta virtuale o stampata che mostra informazioni codificate in un modello grafico in bianco e nero. Nel mondo delle criptovalute, è spesso usato per condividere facilmente gli indirizzi per ricevere fondi.

Race Attack

Livello: avanzato

Argomento: tecnologia

Un attacco di tipo Race Attack è una forma di attacco informatico che sfrutta una vulnerabilità nella gestione delle operazioni concorrenti in un sistema informatico.

Nel caso di Bitcoin, potrebbe essere un double-spend effettuato tramite due transazioni create dagli stessi fondi (UTXO) che vengono inviate in rapida successione e solo una viene confermata nella blockchain. L'obiettivo è acquistare qualcosa con la transazione non confermata per poi invalidarla con una nuova transazione prima che sia confermata.

Viene fatta dall'attaccante ad esempio creando due transazioni in conflitto con UTXO in comune, una fraudolenta verso la vittima e l'altra verso lo stesso attaccante. È sufficiente che l'attaccante sappia che la vittima, ad esempio un

merchant, accetterà la transazione come valida prima che sia confermata, ovvero scritta in un blocco aggiunto alla blockchain, per fornire i beni o servizi.

L'esempio:

L'attaccante crea una transazione tx1 di pagamento alla vittima utilizzando uno o più UTXO in input, con fee sufficientemente basse per fare in modo che la transazione non venga presa in considerazione troppo presto dai miner per essere inserita nel blocco che andranno a minare.

La vittima vede la tx1 in transito (nella mempool), e fornisce comunque all'attaccante i beni o servizi anche se non è stata ancora confermata in blockchain.

L'attaccante a questo punto crea una nuova transazione tx2 con lo stesso o gli stessi UTXO in input della tx1, ma con il pagamento verso se stesso e fee abbastanza alte affinché la tx2 sia scelta dai miner per essere inserita in un nuovo blocco prima della tx1. Una volta che la tx2 è memorizzata nella blockchain, gli input in conflitto vengono considerati spesi e la tx1 viene considerata invalida dai miner e scartata dalla loro transaction pool.

Per evitare un race attack, i merchant devono attendere il completamento del mining e la comparsa della transazione nella blockchain prima di fornire il prodotto/servizio al pagatore, e possibilmente anche un certo numero di conferme, ovvero di blocchi successivi a quello nel quale è presente la transazione. Generalmente viene considerato molto sicuro attendere almeno 6 blocchi successivi come conferma prima di effettuare la consegna di beni o servizi. In questo caso, le possibilità per un attaccante di annullare una transazione sono trascurabili, anche ipotizzando che l'aggressore possa controllare non più del 10% della potenza computazionale totale utilizzata nel mining.

Più recentemente, poiché l'incremento della difficoltà del mining Bitcoin ha reso più proibitivo controllare una percentuale significativa della potenza computazionale, la raccomandazione è di attendere almeno 3 conferme.

Raiden Network

Livello: avanzato

Argomento: tecnologia

Una soluzione di scalabilità off-chain che mira a consentire pagamenti quasi istantanei, a basso costo e scalabili sulla blockchain di Ethereum. È simile al concetto di Lightning Network nella community di Bitcoin.

Ransomware

Livello: base

Argomento: legale

Il ransomware è un tipo di malware utilizzato dagli hacker per rubare o crittografare i file delle loro vittime al fine di estorcere un riscatto in cambio della decrittazione o del ripristino dei file. Il pagamento del riscatto può variare da pochi dollari a milioni, ed è solitamente effettuato in criptovaluta.

I programmi ransomware possono accedere a dispositivi o sistemi in molti modi, più comunemente attraverso schemi di phishing, che arrivano tramite e-mail presentate alle potenziali vittime come file attendibili. Le e-mail di spam contengono spesso link infetti, PDF o altri allegati. Una volta attivati, i programmi ransomware prendono rapidamente il controllo di un dispositivo, mentre l'attaccante ricatta il bersaglio minacciando di distruggere, divulgare o vendere i dati rubati se il riscatto non viene pagato in tempo.

Esistono tre categorie di ransomware:

- **scareware**: si presentano sotto forma di messaggi pop-up che affermano di aver trovato malware nel dispositivo e che l'unico modo per eliminarlo è pagare una certa somma di denaro
- **screen locker**: vengono utilizzati dagli hacker per bloccare l'accesso degli utenti ai loro dispositivi. Non appena i dispositivi vengono avviati, le vittime ricevono un messaggio che sembra provenire dalle forze dell'ordine (FBI, Dipartimento di Giustizia, ecc.), che afferma che sono state rilevate attività illegali sui loro dispositivi o sistemi e che deve essere pagata una multa
- **ransomware encrypting**: vengono utilizzati dagli hacker per bloccare i file di un utente crittografandoli e richiedere un pagamento per la loro decrittazione. Nessun software o strumento di sicurezza può decifrare un file o un sistema crittografato.

Bitcoin sembra essere la forma più popolare di pagamento del riscatto richiesta dagli hacker di ransomware, seguita da Monero per le sue caratteristiche di privacy coin.

RBF

Acronimo di: Replace-by-fee

Livello: intermedio

Argomento: tecnologia

RBF o Replace-by-fee consente di velocizzare la conferma di una transazione aumentando le fee.

È una funzionalità introdotta nel protocollo Bitcoin nel 2015 tramite la proposta BIP 125 che consente ad una transazione di modificare le fee (le commissioni per confermare la transazione) se la transazione è ancora nella mempool e non è stata ancora inserita nella (blockchain.html) Bitcoin.

Capita spesso che ci siano dei periodi nei quali la quantità di transazioni in

attesa di essere incluse nella blockchain è superiore alla disponibilità di spazio nei nuovi blocchi della blockchainblockchain.

Poiché il miner che riesce a minare un nuovo blocco guadagna anche dalle fee delle transazioni, e poiché non tutte le transazioni in attesa potrebbero essere inserite nello spazio limitato di un blocco, il miner andrà a selezionare quelle transazioni che hanno delle fee che gli consentono di guadagnare di più.

Le transazioni competono per essere incluse nel blocco successivo risolto da un miner in base all'importo delle fee o commissione di transazione della rete Bitcoin che la transazione offre di pagare.

Le transazioni la cui fee non è sufficientemente competitiva rimarranno nella mempool, in attesa che i miner eliminino le transazioni che hanno pagato una fee più alta.

I diversi nodi gestiscono la mempool in modo diverso, e possono consentire che le transazioni che si trovano nella loro mempool possano essere modificate o meglio sostituite.

Le modalità RBF possono essere classificate in 2 categorie:

- opt-in RBF, nel quale è l'utente che segnala quando crea la transazione che vuole poter modificare le fee nel caso la transazione
- Full RBF, ovvero il nodo è impostato per consentire la sostituzione della transazione quando ci siano delle condizioni opportune anche se l'utente non ha esplicitamente impostata la transazione come RBF.

Generalmente quando non si esplicita se sia opt-in RBF o Full RBF, si intende opt-in RBF.

Ci sono diversi motivi per si può voler sostituire o meglio aggiornare le transazioni: per aumentare le loro fee, comprimere più transazioni in una sola, creare coinjoin in background (per migliorare la privacy) o eseguire una serie di altre azioni utili.

La possibilità di aumentare le fee di una transazione non ancora confermata è utile sia per fare in modo che venga confermata più velocemente quando ci sono troppe transazioni con fee più convenienti per i miner, che come strategia per pagare fee più basse: se il vostro wallet supporta RBF e tale supporto è abilitato per una transazione, potete scegliere tranquillamente la fascia più bassa della commissione di transazione. Se la transazione non viene confermata abbastanza presto per voi, potete semplicemente aumentare la commissione in un secondo momento utilizzando RBF.

In questo modo, se una transazione ha delle fee più basse rispetto a quelle delle altre transazioni nella mempool, ovvero in attesa di essere inserite dai miner nella blockchain, è possibile creare una transazione che sostituisce quella in attesa con una transazione analoga ma con delle fee più alte per poter essere confermata prima.

È una funzione implementata su molti wallet quali Bitcoin Core, Blockstream Green, Electrum, Samourai Wallet, Specter Wallet, SBW Simple Bitcoin Wallet, Moonshine, Coinb.in, ConIO, Nunchuk e alcuni di questi hanno l'opzione RBF abilitata di default.

RBF ha le seguenti caratteristiche:

- Le transazioni originali non devono essere confermate. Devono indicare la loro sostituibilità in modo esplicito o attraverso l'ereditarietà. Ovvero, se una qualsiasi voce della transazione originale ha un numero di nSequence inferiore a (0xffffff - 1). Oppure, che le transazioni che l'hanno preceduta indichino la sostituibilità (ereditarietà).
- La nuova transazione creata per la sostituzione può includere un input non confermato solo se era incluso nella transazione originale.
- La commissione per la nuova transazione deve essere superiore a quella della transazione originale.
- Quando il numero di transazioni da sostituire non supera le 100 unità.
- La sostituzione delle transazioni è un processo opzionale, anche se alcuni wallet attivano di default RBF

Dalla versione 0.16.0 (febbraio 2018) di Bitcoin Core le transazioni RBF sono diventate un comportamento predefinito (da opt-in a opt-out) e la Transaction replacement, la sostituzione delle transazioni è diventata uno standard de facto sulla rete. Tale cambiamento è stato collegato al limite di 1Mb del blocco e si è reso necessario uno strumento per gli utenti per sostituire le transazioni bloccate. L'attributo più controverso di RBF è che permetteva di inviare fondi a indirizzi assolutamente diversi (full RBF), il che significa praticamente che gli utenti possono fare un double spending con un software standard.

Preserve payment vs Decrease payment Il metodo "Preserve payment" e il metodo "Decrease payment" sono due strategie utilizzate per effettuare RBF.

- **Preserve payment**: (conserva il pagamento) significa che l'importo destinato al destinatario della transazione rimane invariato. Quando utilizzi questa strategia per incrementare la commissione della transazione, il totale inviato al destinatario rimane lo stesso, mentre l'incremento della commissione viene sottratto dal resto che sarebbe tornato al mittente (ovvero, il change).

Esempio:

Transazione originale: invii 1 BTC con una commissione di 0.0001 BTC. Con "Preserve payment": invii sempre 1 BTC al destinatario, ma aumenti la commissione a 0.0005 BTC. La differenza di 0.0004 BTC viene sottratta dal change che tornerebbe al mittente. * **Decrease payment**: (riduci il pagamento) comporta una riduzione dell'importo inviato al destinatario per compensare l'aumento della commissione. In questo caso, l'incremento della commissione viene preso dall'importo destinato al destinatario piuttosto che dal change che tornerebbe

al mittente.

Esempio:

Transazione originale: invii 1 BTC con una commissione di 0.0001 BTC. Con "Decrease payment": aumenti la commissione a 0.0005 BTC, quindi invii 0.9996 BTC al destinatario (diminuito di 0.0004 BTC) mantenendo invariato il change che ritorna al mittente.

Un metodo alternativo per velocizzare la conferma di una transazione è CPFP Child pays for parent, la cui differenza principale è data dal caso d'uso perché con RBF è chi effettua il pagamento che può accelerarne la conferma modificando le fee, mentre con CPFP è il ricevente che creando una transazione che spende i bitcoin della transazione non ancora confermata che può incentivare i miner.

La differenza con CPFP può quindi essere così riassunta:

- RBF consente al mittente di incrementare le fee per ottenere la conferma della transazione più velocemente. Utilizzate RBF se siete il mittente che ha bisogno di velocizzare la transazione.
- CPFP consente al destinatario creando una nuova transazione di pagare per ottenere la conferma della transazione più velocemente. Usate il CPFP se siete il destinatario che ha bisogno di velocizzare la transazione.

Un funzionamento alternativo al RBF è il FSS o First-Seen-Safe, secondo il quale i nodi della rete bitcoin quando ricevono nuove transazioni controllano se nella mempool c'è già un'altra transazione che spende lo stesso UTXO, e nel caso in cui tale transazione venga trovata, la nuova viene rifiutata e non viene inclusa nel mempool di questo nodo e non viene propagata ulteriormente alla rete.

Rebound

Rimbalzo

Livello: intermedio

Argomento: finanza

un rimbalzo si riferisce a un recupero da un periodo precedente di attività o perdite negative. Nel contesto di azioni o criptovalute, un rimbalzo significa che il prezzo è aumentato da un livello inferiore. Il rimbalzo è un movimento rialzista di un titolo generalmente provocato da una tenuta di un supporto.

Redeem Script

Livello: avanzato

Argomento: tecnologia

Un RedeemScript è lo script utilizzato per sbloccare i bitcoin inviati a un indirizzo P2SH o P2WSH. In una transazione P2SH o P2WSH, i bitcoin sono bloccati sull'hash di un RedeemScript, garantendo che solo qualcuno che può riprodurre il RedeemScript e aggiungere le firme richieste possa spendere i bitcoin. I Redeem Script di solito implicano script multisig o script wrapped SegWit

regtest

Livello: avanzato

Argomento: tecnologia

La modalità Regtest, abbreviazione di "Regression Test", è una modalità utilizzata dagli sviluppatori di Bitcoin per testare il loro codice in un ambiente isolato. Si può pensare a regtest come a una blockchain Bitcoin privata di test che funziona in modo molto simile alla testnet Bitcoin, ma con alcune particolarità:

- Ambiente isolato: Regtest non è connesso alla rete Bitcoin reale. Ciò significa che qualsiasi transazione o modifica effettuata su regtest non ha alcun effetto sulla rete principale o sulle testnet o regtest di altri utenti.
- Generazione rapida di blocchi: Gli sviluppatori possono generare rapidamente nuovi blocchi su regtest, il che consente loro di testare rapidamente come il loro codice reagisce a diversi scenari.
- Monete senza valore: le monete create su regtest non hanno alcun valore reale e non possono essere utilizzate sulla rete principale di Bitcoin; dovrebbe essere così anche con la testnet anche se ci sono dei casi che hanno portato alle monete testnet ad essere commercializzate

Per le situazioni in cui l'interazione con peer e blocchi casuali non è necessaria o indesiderata, la modalità di test di regressione di Bitcoin Core consente di creare istantaneamente una nuovissima catena di blocchi privata con le stesse regole di base di testnet, ma con una differenza importante: tu scegli quando creare nuovi blocchi, così hai il controllo completo sull'ambiente.
Molti sviluppatori considerano la modalità regtest il modo preferito per sviluppare nuove applicazioni.

Rekt

Livello: base

Argomento: finanza

Storpiatura della parola wrecked (che significa rovinato, distrutto o gravemente danneggiato), il termine deriva dai videogiochi, dove indica che un giocatore è stato completamente distrutto, solitamente usato nei giochi sparatutto in prima persona. Nelle criptovalute, qualcuno è rekt se subisce una perdita a causa di un

cattivo investimento in criptovalute. Si potrebbe anche dire che una criptovaluta che è scesa in modo significativo di valore è rekt.

relay network

Livello: avanzato

Argomento: tecnologia

Sebbene la rete P2P bitcoin soddisfi le esigenze generali di un'ampia varietà di tipi di nodi, mostra una latenza di rete troppo elevata per le esigenze specializzate dei nodi di mining bitcoin.

I miner Bitcoin sono impegnati in una competizione a tempo per risolvere il problema della Proof-of-Work per aggiungere nuovi blocchi alla blockchain. Durante la partecipazione a questa competizione, i miner bitcoin devono ridurre al minimo il tempo tra la propagazione di un blocco vincente e l'inizio del prossimo round di competizione. Nel mining, la latenza di rete è direttamente correlata ai margini di profitto.

Una Relay Network Bitcoin è una rete che tenta di ridurre al minimo la latenza nella trasmissione di blocchi tra miner.

Le relay network non sostituiscono la rete P2P di bitcoin. Si tratta invece di reti overlay che forniscono connettività aggiuntiva tra nodi con esigenze specializzate. Poiché le autostrade non sostituiscono le strade rurali, ma piuttosto scorciatoie tra due punti con traffico intenso, sono comunque necessarie piccole strade per collegarsi alle autostrade.

La Relay Network Bitcoin originale è stata creata dallo sviluppatore Matt Corallo nel 2015 per consentire una rapida sincronizzazione dei blocchi tra miner con una latenza molto bassa. La rete era composta da diversi nodi specializzati ospitati sull'infrastruttura di Amazon Web Services in tutto il mondo e serviva per collegare la maggior parte dei miner e dei mining pool.

La Relay Network iniziale di Bitcoin originale è stata sostituita nel 2016 con l'introduzione di FIBRE, Fast Internet Bitcoin Relay Engine.

Remittance

Rimessa

Livello: intermedio

Argomento: politica

Le rimesse, remittance in inglese, sono trasferimenti di denaro da una persona all'altra, spesso effettuati da lavoratori emigrati ai propri parenti.
Nel linguaggio bancario e commerciale, si riferisce alla trasmissione di fondi, titoli o valori da una persona all'altra.

In particolare, indica il pagamento che un debitore invia al creditore per regolare un debito in valuta estera.

Sono pagamenti effettuati da un luogo all'altro e, nella maggior parte dei casi, comportano il trasferimento di capitale da parte di un individuo a un contatto estero, come nel caso di un lavoratore straniero che invia denaro a un parente o conoscente nel proprio paese d'origine.
Tradizionalmente, questi pagamenti vengono effettuati tramite fornitori di servizi che operano non solo online, come MoneyGram e Western Union.

Con l'avvento delle criptovalute, le attività di rimesse hanno visto grandi vantaggi e opportunità nell'utilizzo di questi sistemi: spesso sono più rapide ed economiche rispetto a quelle effettuate attraverso il sistema bancario tradizionale. Le persone possono ora trasferire importi molto piccoli o molto grandi con la stessa semplicità, essenzialmente in qualsiasi parte del mondo, in pochi secondi, sostenendo commissioni minime e senza dover sottostare a censure o altri blocchi dei sistemi finanziari tradizionali.

Reorg

Acronimo di: Chain reorganization

Riorganizzazione della catena

Livello: intermedio

Argomento: tecnologia

Una Chain reorganization o Blockchain reorganization, riorganizzazione della catena spesso abbreviata in **Reorg**, si verifica quando l'ultimo o gli ultimi blocchi vengono rimossi dalla blockchain per essere sostituiti da quella che viene considerata una catena più lunga, longest chain.

Di solito una riorganizzazione della catena avviene quando due blocchi vengono minati più o meno contemporaneamente. A causa della velocità di propagazione dei blocchi attraverso la rete, alcuni nodi riceveranno prima un blocco e alcuni nodi riceveranno prima l'altro blocco. Pertanto ci sarà un disaccordo su quale di questi blocchi sia da considerare come valido per far proseguire la blockchain. Si crea quindi una biforcazione, o fork, della blockchain e i miner aggiungeranno i nuovi blocchi ad uno dei rami del fork. Per considerare quale ramificazione sia valida i nodi utilizzeranno la regola della catena più lunga, e scarteranno i blocchi del ramo della catena più corta. I blocchi scartati vegono chiamati orphan blocks, blocchi orfani.

La catena più lunga viene calcolata come quella per la quale è stato utilizzato il maggior calcolo.

Una reorg potrebbe essere il risultato di un selfish mining attack.

Replacement cycling vulnerability

Livello: avanzato

Argomento: tecnologia

La Replacement cycling vulnerability è una vulnerabilità che può consentire, in presenza di determinate condizioni, di far effettuare un attacco contro chi gestisce canali lightning network con potenziale perdita di fondi.

Sono interessati solo i nodi che utilizzano i canali lightning per effettuare il routing di pagamenti su lightning network.

Gli utenti che utilizzano i propri canali solo per effettuare e ricevere pagamenti non sono interessati.

Dopo la divulgazione della vulnerabilità, sono stati effettuati degli aggiornamenti delle implementazioni dei nodi lightning network per includere mitigazioni per l'attacco.

Il termine replacement si riferisce al Transaction replacement, o Sostituzione della transazione, ovvero alla possibilità di sostituire una transazione nella mempool prima che questa venga confermata nella block chain.

È possibile utilizzare la sostituzione della transazione per rimuovere uno o più input di una transazione multi-input dalla mempool.
Come esempio, un attaccante malintenzionato che chiamiamo Mallory trasmette una transazione con due input, che spendono gli utxo A e B.
Successivamente Mallory sostituisce quella transazione con una versione alternativa con un unico input che spende solo l'utxo B. Dopo questa sostituzione, l'utxo A e tutti i dati in esso inclusi sono stati rimossi dalle mempool di ogni nodo che ha elaborato la sostituzione.
Mallory può sfruttare questo comportamento se vuole rimuovere un input dalla mempool dei nodi.
In particolare, se Mallory condivide il controllo su un output con un utente vittima dell'attacco che chiamiamo Bob, può aspettare che Bob spenda l'output, sostituire la sua spesa con una sua spesa che contenga un input aggiuntivo e quindi sostituisca la sua spesa con una transazione che non spende più il loro risultato condiviso.
Questo è un replacement cycle, un ciclo di sostituzione.
I miner continueranno a riscuotere le commissioni di transazione da Mallory, ma c'è un'alta probabilità che né le spese di output di Bob né quelle di Mallory vengano confermate in prossimità del momento in cui Bob trasmette la sua spesa.
Questo comportamento che possiamo considerare una vulnerabilità è particolarmente importante nel caso ad esempio di Lightning Network che utilizza gli HTLC Hash Time-Locked Contract, ma anche di altri protocolli, perché determinate transazioni devono avvenire entro determinate finestre temporali per garantire che gli utenti che inoltrano i pagamenti non perdano denaro.

Replay Attack

Livello: intermedio

Argomento: tecnologia

È un tipo di attacco che può avvenire in concomitanza di una chain split della blockchain.

Quando avviene una chain split a causa di un fork la blockchain si divide in due rami, in cui le chiavi private associate alla criptovaluta relativa a quel network sono comuni ai due rami e possono generare transazioni valide su entrambi.

Se, a valle del fork, si effettuasse una transazione sulla catena A, l'utente che riceve i fondi può prendere la transazione e trasmetterla sulla catena B ricevendo i fondi anche sulla catena B anche se la transazione non è stata trasmessa da chi ha creato la transazione.

Per evitare questo rischio, quando si genera un fork che produce una chain split, la nuova cripto che genera lo split dovrebbe attivare nelle sue regole un meccanismo di protezione chiamato reply protection.

Questo fu infatti ciò che successe nel 2016 all'exchange Coinbase quando ci fu il fork di Ethereum e Ethereum Classic: inizialmente Coinbase era vulnerabile al replay attack. Nei primi giorni dopo la separazione, quando si prelevava Ethereum da Coinbase, c'era la possibilità che Coinbase inviasse due versioni della transazione: una su Ethereum e una su Ethereum Classic. Alcuni sofisticati trader del settore furono in grado di capitalizzare questa svista di Coinbase: potevano dividere le loro monete in Ethereum Classic ed Ethereum, poi depositare Ethereum su Coinbase. Senza fare trading, gli Ethereum appena caricati potevano essere ritirati da Coinbase e il trader poteva sperare di fare replay e di ricevere Ethereum Classic gratuitamente. Dopo un certo periodo, Coinbase scoprì l'errore e implementò una forma di replay protection e coprì le perdite con il proprio bilancio.

Reproducible

Riproducibile

Livello: avanzato

Argomento: tecnologia

Il software Reproducible, o Riproducibile, è un software Open Source che la caratteristica non solo di rendere pubblicamente visibile il suo codice sorgente, ma anche la possibilità per un utente di creare dal sorgente il programma in autonomia.

Il concetto di "riproducibilità" in informatica si riferisce alla possibilità di generare una replica esatta di un software a partire da un insieme noto di input, in

particolare dal suo codice sorgente. Se è possibile ricostruire esattamente il software scaricato a partire dal codice sorgente pubblico, con tutti i byte verificati, allora si può dire che il software è riproducibile. Tuttavia, questo non significa che il codice sia stato verificato, ma solo che è la premessa per garantire che il codice sorgente pubblico sia corrispondente al software fornito.

Avere un software riproducibile significa che gli utenti possono verificare che il prodotto rilasciato sia basato sul codice noto a tutti gli sviluppatori del team e che i ricercatori in sicurezza possono verificare se il fornitore mette a rischio i loro fondi. Inoltre, un eventuale truffatore dovrebbe fare maggiori sforzi per nascondere eventuali exploit.

È importante notare che "riproducibilità" non significa "verifica". Ci sono buone ragioni per credere che i ricercatori in sicurezza di oggi potrebbero non rilevare backdoors ovvi nel codice sorgente pubblico prima che vengano sfruttati, e ancor meno se l'attaccante fa sforzi moderati per nasconderli. Ciò è particolarmente vero per i progetti meno popolari.

Nel caso dei software Bitcoin quali nodi e wallet questa è una caratteristica molto importante perché oltre le garanzie date dall'open source, è possibile produrre in autonomia il programma dal sorgente garantendo in questo modo che nel processo di compilazione e distribuzione non siano introdotte ad arte o in modo inconsapevole delle alterazioni che possono compromettere la sicurezza e quindi consentire furti e attacchi ai fondi degli utenti.

Resistance

Resistenza

Livello: base

Argomento: finanza

In ambito finanziario, la resistenza è un livello di prezzo al quale un asset, come Bitcoin, tende a trovare una pressione di vendita che impedisce ulteriori aumenti del prezzo.
Questo livello agisce come un "tetto" causato da un'elevata quantità di vendite in quell'area di prezzo, creando una barriera difficile da superare senza una significativa pressione di acquisto.

Gli analisti tecnici tracciano le linee di resistenza in base ai massimi precedenti per prevedere potenziali punti di inversione dei prezzi. Questi livelli sono generalmente rappresentati come linee orizzontali, ma possono anche essere diagonali, nel qual caso sono chiamate linee di tendenza. Un livello di resistenza superato tende a diventare un livello di supporto, che svolge la funzione opposta: agisce come un "pavimento" che impedisce al prezzo di scendere ulteriormente.

La resistenza può essere identificata esaminando un portafoglio ordini, dove i livelli di prezzo con un grande numero di ordini di vendita in sospeso indicano potenziali resistenze. Può anche essere determinata dai movimenti storici dei

prezzi e può manifestarsi come un prezzo costante o una linea di tendenza variabile nel tempo. La comprensione dei livelli di resistenza è cruciale per i trader attivi, poiché offre indicazioni su possibili punti di ingresso o uscita dal mercato e opportunità di trading quando tali livelli vengono infranti.

Retarget

Livello: intermedio

Argomento: tecnologia

Il retarget, o Difficulty Adjustment, è la regolazione della difficoltà per i miner.

Il retarget o retargeting, indicato anche come Difficulty adjustment o correzione della difficoltà, è la modifica del Target Hash utilizzato nella Proof-of-work per fare in modo che al variare dell'Hash rate la difficoltà sia tale da garantire un tempo medio di 10 minuti per generare un nuovo blocco.

I nodi partecipanti alla rete Bitcoin ogni 2016 blocchi minati verificano se i nuovi blocchi vengono generati in media uno ogni 10 minuti.

Poiché la capacità di trovare nuovi blocchi si basa sulla potenza di calcolo utilizzata dai miner o Hash Rate, ci possono essere diversi eventi che fanno in modo che l'Hash Rate possa crescere o diminuire.

Di solito, l'Hash rate aumenta: si aggiungono nuovi miner alla rete Bitcoin, attirati dall'opportunità di guadagno, e vengono immessi sul mercato hardware di mining con maggiore potenza di calcolo. Questo fa in modo che i blocchi vengano minati più velocemente.

Ci sono anche dei casi nei quali l'Hash rate diminuisce: ad esempio nel 2021 i miner cinesi per motivi normativi hanno dovuto interrompere o spostare le loro attività, causando una forte diminuzione dell'Hash rate. Un altro motivo per la diminuzione dell'Hash rate può essere dovuto ad un Bear market che rende meno profittevole il mining fino a compromettere i bilanci dei miner costringendoli a spegnere le loro macchine o addirittura a chiudere.

Il retargeting viene calcolato dividendo il Target hash del primo blocco per il Target hash del blocco corrente.

RGB

Livello: avanzato

Argomento: tecnologia

RGB è una suite di protocolli per smart contract scalabili e riservati per Bitcoin e Lightning Network.
Consente di gestire concetti quali di proprietà privata e reciproca, astrazione e separazione dei commitment e rappresentano la "post-blockchain", una forma

Turing completa di elaborazione distribuita senza fiducia che non richiede l'introduzione di "token".

Essendo un sistema di smart contract, RGB è molto diverso dagli approcci precedenti, sia basati su Bitcoin come Colored coins, Counterparty, OMNI che non-bitcoin (Ethereum, EOS e altri): separa il concetto di state owners e state evolution, mantiene il codice dello smart contract e i dati offchain, utilizza la blockchain come un layer di state commitment e Bitcoin script come sistema di controllo della proprietà; mentre l'evoluzione dello smart contract è definita dallo schema off-chain.

La nascita di RGB risale al 2016, quando Peter Todd introdusse la nozione di sigillo monouso e CSV (client side validation, validazione lato cliente). Costruito su questi concetti critici, RGB fu proposto nel 2018.

Nel 2019, Orlovsky, un sviluppatore centrale di RGB, guidò il suo sviluppo e creò molti componenti che alla fine costituiscono il protocollo RGB. Inoltre, l'istituzione dell'Associazione LNP/BP in Svizzera ha contribuito a fornire gli standard. Dopo ampi sforzi di sviluppo, RGB ha presentato la sua versione v0.10 nell'aprile 2023.
La prima versione stabile di RGB, con versione v0.10, è stata pubblicata all'inizio di settembre 2023, con la disponibilità del tool a linea di comando e della libreria runtime per l'integrazione su desktop e dispositivi mobili.

La libreria è stata ampiamente testata da diverse squadre indipendenti e alimenta tre diversi wallet (MyCitadel su Desktop, Iris su Android, BitMask sul Web).

RGB separa il concetto dell'emittente dello smart contract, owner dello stato ed evoluzione dello stato, mantiene codice e dati dello smart contract off-chain, e utilizza la block chain come layer per il commitment dello stato e Bitcoin script come sistema di controllo dell'ownership e l'evoluzione degli smart contract viene definita off-chain.

Gli emittenti possono utilizzare gli schemi RGB, che fungono da modelli di contratti che possono essere utilizzati per casi d'uso specifici.

Ecco alcuni esempi:

- RGB20 Emissione di asset fungibili
- RGB21 Emissione di asset non fungibili
- RGB22 Identità digitali decentralizzate
- RGB23 Registro storico unico verificabile per dati auditabili
- RGB24 Sistema di nomi di dominio globale decentralizzato
- RGB25 Emissione di asset collezionabili

RGB 20 Tra le feature supportate dallo standard RGB 20:

- emissione secondaria trasparente;
- emissione di un report e massima offerta;

- funzionalità di proof of reserve;
- supporto alla suddivisione di azioni;
- funzionalità componibili ed espandibili tramite ereditarietà di interfaccia.

Tra gli asset già emessi su RGB esistono USDN e BTCN, i quali rappresentano rispettivamente USDT e BTC.

Chiunque è libero di sviluppare il proprio schema per diverse applicazioni senza dover chiedere il permesso agli sviluppatori di RGB. Tuttavia, si prevede che la maggior parte dei casi d'uso possa essere coperta con pochi schemi principali.

RGB utilizza AluVM (algorithmic logic unit virtual machine), una macchina virtuale RISC basata su registri appositamente progettata.
AluVM è Turing-completa e può operare lo stato globale con le stesse garanzie di disponibilità dei sistemi esistenti basati su blockchain.
Come EVM, AluVM presenta un'architettura che annida un nodo RGB sulla Lightning Network, ospitando un cliente RGB in nodi RGB.

Confronto di RGB con TARO TARO (ora Taproot Assets), un protocollo supportato da Taproot, è stato presentato da Lightning Labs ed è in fase di sviluppo.

Sia RGB che TARO si basano su CSV.
Poiché i due condividono design simili, alcuni addirittura sostengono che TARO si sia ispirato a RGB. Tuttavia, ora sembra che si concentrino su aspetti diversi: TARO si concentra sui token, mentre RGB intende implementare funzioni di smart contract.

ring of fire

Livello: avanzato

Argomento: tecnologia

Un Ring of Fire è una comunità online con un unico grande obiettivo da raggiungere: connettere nodi di lightning da ogni parte del mondo.

Nel luglio 2021 è stato creato il più grande Ring of Fire fino ad oggi, con 65 nodi partecipanti e 65.000.000 di sat di liquidità.

RIPEMD

Livello: avanzato

Argomento: tecnologia

RIPEMD (RACE Integrity Primitives Evaluation Message Digest) è un algoritmo di hash utilizzata da Bitcoin.

In particolare viene utilizzata la versione RIPEMD-160 che genera in output un hash di 160 bit.

Il RIPEMD originale, così come RIPEMD-128, non è considerato sicuro perché il risultato a 128 bit è troppo piccolo e anche (per il RIPEMD originale) a causa di punti deboli di progettazione.
Le versioni a 256 e 320 bit di RIPEMD forniscono rispettivamente lo stesso livello di sicurezza di RIPEMD-128 e RIPEMD-160; sono progettati per applicazioni in cui il livello di sicurezza è sufficiente ma è necessario un risultato hash più lungo.

In Bitcoin, RIPEMD-160 viene utilizzato per due scopi principali:

- Per creare indirizzi Bitcoin. L'indirizzo Bitcoin è una stringa alfanumerica di 34 caratteri che identifica un portafoglio Bitcoin. Viene generato hashando il pubkey del portafoglio con RIPEMD-160.
- Per verificare le firme digitali Bitcoin. Le firme digitali Bitcoin vengono utilizzate per verificare le transazioni. Vengono generate hashando il messaggio da firmare con SHA-256 e quindi hashando l'output con RIPEMD-160.

La scelta di utilizzare due funzioni di hash è dovuta al fatto che SHA-256 è una funzione di hash più robusta, ma produce un output di 256 bit, che è troppo lungo per essere utilizzato come indirizzo Bitcoin. RIPEMD-160, invece, produce un output più breve, ma comunque sufficientemente unico per identificare un portafoglio Bitcoin.

ROI

Acronimo di: Return on investment

Ritorno sull'investimento

Livello: base

Argomento: economia

Ritorno sull'investimento o indice di redditività del capitale investito. Il termine indica il guadagno sul capitale investito, cioè quanto (in punti percentuali) ha fruttato l'investimento iniziale.

Rollup

Livello: avanzato

Argomento: tecnologia

Un Rollup è una soluzione di tipo layer 2, nate inizialmente come soluzioni di scaling per permettere di gestire un gran numero di transazioni al di fuori della blockchain principale (Layer 1) in modo più efficiente ed economico, senza congestionare la blockchain principale e senza compromettere la sicurezza e la decentralizzazione della rete, e che ora i membri della comunità Bitcoin stanno

iniziando a esplorare come indirizzare più casi d'uso, utenti e entrate derivanti dalle commissioni verso Bitcoin.

In pratica, un rollup raccoglie un gran numero di transazioni effettuate al di fuori della blockchain principale, le elabora e le comprime in un singolo blocco, che viene poi pubblicato sulla blockchain principale. In questo modo, invece di registrare ogni singola transazione sulla blockchain principale, che richiederebbe molto tempo e risorse computazionali, un rollup può registrare molte transazioni in un solo colpo, riducendo i tempi di elaborazione e i costi.

Esistono diversi tipologie di rollup, tra cui:

- Zk-Rollup o rollup a conoscenza zero,
- Optimistic Rollup, che si differenziano per il modo in cui gestiscono la sicurezza e la privacy delle transazioni al di fuori della blockchain principale.
- Validity rollup
- Sovereign rollup

Validity rollup Un rollup di validità è una blockchain che utilizza prove di validità per dimostrare il suo stato aggiornato al Livello 1. Le prove di validità sono prove crittografiche che prendono i dati della transazione dal rollup, comprimono i dati della transazione all'interno della prova e dimostrano la correttezza del cambiamento di stato proposto al Livello 1.
In Ethereum, lo stato di validità del rollup è mantenuto da un contratto intelligente nel Livello 1.
Gli utenti eseguono una serie di transazioni offchain, i dimostratori prendono quelle transazioni e riassumono come tali transazioni cambiano lo stato della blockchain, e una prova di validità dimostra che la sintesi è vera.

Sovereign rollup Un Sovereign rollup è una blockchain che utilizza una blockchain di livello 1 per la disponibilità dei dati, ma non per il settlement.
I nodi in un consolidamento sovrano sono responsabili della verifica della correttezza dei cambiamenti di stato.
In questo modello, essi leggerebbero una prova di validità contenente un cambiamento di stato e verificherebbero che l'esecuzione sia stata effettuata correttamente.
Questo è vantaggioso per le blockchain che desiderano esplorare senza fiducia diversi ambienti di esecuzione e funzionalità, ma che vogliono comunque ereditare la sicurezza di un protocollo decentralizzato di Livello 1.
Ci sono anche differenze nel modo in cui aggiornano il loro protocollo rispetto ai consolidamenti di validità.

Zk-Rollup Una prova a conoscenza zero (zkp) è una prova crittografica che consente di dimostrare che un'affermazione è vera senza rivelarla per intero.
Nel contesto delle blockchain, vengono utilizzate principalmente per la privacy e il ridimensionamento. Nella privacy, gli zkps dimostrano che le transazioni sono

valide senza rivelare informazioni sugli utenti impegnati in una transazione. Nel ridimensionamento, gli zkps dimostrano che un lotto di transazioni è realmente il risultato di una proposta di cambiamento di stato.

Bitcoin rollup Sebbene Satoshi Nakamoto avesse teorizzato le zero-knowledge-proof, e la prima proposta concreta in contesto Bitcoin sia stata avanzata nel 2011 da Greg Maxwell, uno dei principali developer Bitcoin, le soluzioni Rollup si sono sviluppate principalmente per la blockchain Ethereum, ma proseguono studio, verifica e proposte di implementazioni su blockchain Bitcoin.
Le rollup su Bitcoin sono nuovi fenomeni introdotti da Trey Del Bonis e ulteriormente studiati da John Light. A causa dei compromessi fatti per garantire la decentralizzazione del protocollo Bitcoin, è necessario utilizzare soluzioni offchain per aumentare la quantità di transazioni che può elaborare in modo efficiente. I rollup sono soluzioni di scalabilità popolari nello spazio Ethereum e ora vengono sviluppati utilizzando il protocollo Bitcoin per la disponibilità dei dati. I rollup sviluppati oggi su Bitcoin sono rollup sovrani e rollup verificati ottimisticamente tramite BitVM.

Round Amounts Heuristic

Livello: avanzato

Argomento: legale

La Round Amounts Heuristic, euristica degli importi tondi, nota anche come Change Output Heuristic, è una tecnica utilizzata nella Chain Analysis di transazioni per identificare gli indirizzi Bitcoin che potrebbero essere utilizzati da un utente per ricevere pagamenti non professionisti.

Questa tecnica si basa sul principio che le transazioni di Bitcoin che coinvolgono importi arrotondati, ad esempio 0,1 BTC o 1 BTC, potrebbero essere state effettuate da utenti che non hanno familiarità con i meccanismi di trasferimento di Bitcoin. Al contrario, le transazioni che coinvolgono importi non arrotondati potrebbero essere state effettuate da utenti più esperti o da bot o exchange.

La Round Amounts Heuristic è spesso utilizzata in combinazione con altre tecniche di Chain Analysis per identificare gli indirizzi utilizzati da un utente per ricevere pagamenti, e aiuta a migliorare l'accuratezza delle analisi.

Viene utilizzata per cercare di determinare quali output di una transazione stanno inviando a un'altra parte e quali stanno restituendo bitcoin al mittente come resto. Questa euristica analizza gli importi di ciascun output per effettuare una determinazione. Come tutte le euristiche di Chain Analysis, l'euristica Round Amounts è probabilistica: non può offrire certezza.

Ad esempio, se una transazione crea due output di 0,6 BTC e 0,04543245 BTC, si può ipotizzare che l'output di 0,8 BTC sia stato inviato a un'altra parte come pagamento, mentre il secondo output era l'output di resto, o Change output.

Allo stesso modo, se l'importo di un output in bitcoin è convertibile in un importo preciso e rotondo in una valuta fiat come il dollaro USA, si potrebbe presumere che si tratti di un pagamento e non di un output di resto, anche se le oscillazioni di prezzo e le differenze di quotazioni aumentano l'incertezza su questo indicatore.

Route blinding

Livello: avanzato

Argomento: tecnologia

Il route blinding è una tecnica per aumentare la privacy delle transazioni Lightning Network.

Route blinding consente a un destinatario di un pagamento Lightning di fornire un blinded route, un percorso cieco, ai potenziali pagatori. Ciascun node_id del percorso viene mascherato e possono essere inclusi dei dummy hop (salti fittizi).

Route blinding consente ad un nodo di ricevere un pagamento o un messaggio onion senza rivelare la propria identità al pagatore o al mittente. Non è necessario rivelare altre informazioni direttamente identificabili.
Il route blinding funziona facendo scegliere al ricevente gli ultimi diversi hop attraverso i quali il pagamento o il messaggio verranno inoltrati. Questi passaggi sono crittografati a cipolla come le informazioni di inoltro regolari e vengono forniti al pagatore o al mittente che li utilizza per inviare un pagamento al primo hop. Quel hop inizia il processo di decrittazione dell'hop successivo, inoltrando il pagamento ad esso, facendo decrittare il hop successivo, ecc., fino a quando il ricevente accetta il pagamento senza che il suo nodo venga rivelato al pagatore o al mittente.

Si tratta di un'alternativa al rendezvous per preservare l'anonimato del destinatario.
Ha una serie di compromessi diversi: le onion routing sono riutilizzabili, ma le garanzie di privacy sono un po' più deboli e richiedono più lavoro (ad esempio per la gestione degli errori).

Route blinding è stato descritto per la prima volta nella newsletter Bitcoin Optech a febbraio 2020.

Routing

Instradamento

Livello: avanzato

Argomento: tecnologia

Il routing nel networking si riferisce al processo di trasmissione dei dati tra reti o sottoreti. Quando un dispositivo in una rete invia dati a un altro disposi-

tivo, i dati devono effettuare l'attraversamento di nodi della rete, genericamente definiti router, per raggiungere la loro destinazione.

Il routing su Bitcoin può riferirsi:

- al processo di instradamento delle transazioni e dei blocchi attraverso la rete dei nodi Bitcoin
- al routing su Lightning Network, il processo di instradamento dei pagamenti sui canali Lightning Network

Il processo di routing inizia quando un utente crea una transazione Bitcoin e la trasmette ai nodi della rete Bitcoin, che la verificano e la trasmettono ad altri nodi, e fintanto che non è confermata viene mantenuta nell'area di transito chiamata mempool.
I miner prelevano dalla mempool un certo numero di transazioni per poterle inserire in un blocco, validare il blocco inserendolo nella blockchain. I full node mantengono una copia della blockchain, instradando tra di loro i blocchi confermati.

Il routing su Bitcoin è gestito principalmente dal protocollo di rete Bitcoin e dai software dei nodi che operano sulla rete.

RPOW

Acronimo di: re-usable proof-of-work

Livello: avanzato

Argomento: economia

RPOW, Reusable Proof-of-Work, è stato inventato da Hal Finney come prototipo per una moneta digitale basata sulla teoria dei collezionabili di Nick Szabo.
RPOW rappresentava un passo significativo nella storia del denaro digitale ed è stato un precursore di Bitcoin. Sebbene non fosse destinato a diventare più di un prototipo, RPOW era un software molto sofisticato che avrebbe potuto servire una vasta rete, se avesse avuto successo.

Contesto Storico Negli anni '90, i Cypherpunks iniziarono a esplorare l'idea di una moneta digitale il cui valore non dipendesse da un'organizzazione emittente. Seguendo Nick Szabo, questa forma di denaro digitale doveva essere riconoscibile come limitata in fornitura e quindi utilizzabile come denaro, essendo provabilmente difficile da creare. Questo poteva essere realizzato definendo le unità della moneta digitale in termini di proof-of-work. Alcune proposte per collezionabili digitali circolavano nella mailing list dei cypherpunk, tra cui b-money di Wei Dai e Bit Gold di Nick Szabo. RPOW è stato l'unico collezionabile digitale a funzionare effettivamente come software.

Funzionamento Un client RPOW crea un token RPOW fornendo una stringa di proof-of-work di una determinata difficoltà, firmata con la propria chiave privata. Il server registra quindi il token come appartenente alla chiave firmataria. Il client può successivamente trasferire il token a un'altra chiave pubblica firmando un ordine di trasferimento. Il server aggiorna il registro, assegnando la proprietà del token alla chiave privata corrispondente.

Il problema della doppia spesa è una sfida fondamentale per ogni valuta digitale. RPOW lo risolve mantenendo un registro delle proprietà dei token su un server fidato. Tuttavia, il design di RPOW includeva un modello di sicurezza avanzato per rendere il server più affidabile di una banca tradizionale. I server RPOW erano progettati per operare su processori crittografici sicuri IBM 4758, in grado di verificare in modo sicuro l'hash del software in esecuzione. Inoltre, i server RPOW potevano cooperare tra loro per gestire un numero maggiore di richieste.

RSI

Acronimo di: Relative Strength Index

Indice di forza relativa

Livello: intermedio

Argomento: economia

Una forma di analisi tecnica che funge da "oscillatore del momento", misurando la velocità e il cambiamento dei movimenti dei prezzi, sviluppato da J. Welles Wilder. Oscilla tra zero e 100: una criptovaluta viene considerata iper comprata (overbought) quando l'indicatore è superiore a 70 e iper venduta (oversold) se inferiore a 30. Il RSI è un oscillatore esperto basato sul momentum che viene utilizzato per misurare la velocità e il cambiamento (ampiezza) dei movimenti direzionali dei prezzi. In sostanza, l'RSI, se rappresentato graficamente, fornisce un mezzo visivo per monitorare sia i punti di forza che quelli di debolezza attuali e storici di un particolare mercato. La forza o la debolezza si basa sui prezzi di chiusura per la durata di un periodo di trading specificato, creando una metrica affidabile delle variazioni di prezzo e momentum. L'RSI ha dimostrato di essere un valido indicatore dei movimenti dei prezzi.

Rug Pull

Livello: base

Argomento: legale

Una rug pull è una truffa nel settore delle criptovalute in cui i creatori di un progetto di criptovaluta o di token abbandonano il progetto e si prendono tutti i soldi degli investitori.

Il termine “rug pull”, in italiano tiro del tappeto, deriva dall’immagine di qualcuno che tira il tappeto da sotto i piedi di qualcun altro, lasciandolo cadere.
Nel caso delle criptovalute, questo significa che i creatori del progetto attirano gli investitori con promesse di guadagni elevati, ma poi ritirano tutti i soldi e scompaiono.

I rug pull di solito si verificano nell’ecosistema della finanza decentralizzata (DeFi), in particolare negli scambi decentralizzati (DEX), in cui individui malintenzionati ad esempio creano un token e lo listano su un DEX, quindi lo abbinano a una criptovaluta leader come Ethereum. Una volta che una quantità significativa di investitori ignari ha scambiato il proprio ETH con il token elencato, i creatori ritirano tutto dal pool di liquidità, portando il prezzo della moneta a zero.

I creatori della moneta potrebbero persino creare un clamore temporaneo utilizzando piattaforme di social media come a Telegram, X (ex Twitter), Discord e altre e inizialmente iniettando una certa quantità di liquidità nel loro pool per alimentare la fiducia degli investitori.

I rug pull sono spesso difficili da rilevare perché i creatori dei progetti di criptovalute possono essere molto convincenti. Possono creare siti web e social media accattivanti, e possono fare promesse di guadagni elevati che sono difficili da resistere.

Questo tipo di truffe prospera sui DEX perché questi tipi di scambi consentono agli utenti di elencare i token gratuitamente e senza controllo.

Alcuni segnali che possono indicare una rug pull possono essere: * Promesse di guadagni elevati e rapidi: Se un progetto promette rendimenti incredibilmente alti e in tempi molto brevi, è probabile che sia una truffa. Gli investimenti legittimi comportano rischi, e le promesse di ricchezza istantanea dovrebbero essere viste con sospetto. * Il progetto non ha un piano di sviluppo chiaro o realistico. * Whitepaper e documentazione incoerenti o scarsi: Un progetto legittimo di solito avrà un whitepaper dettagliato che spiega la tecnologia, il caso d’uso e il piano di sviluppo. Se la documentazione è scarna o contiene informazioni vaghe, potrebbe essere un segno di una truffa. * Anonimato degli sviluppatori: Se i membri del team di sviluppo o i promotori del progetto, ancor più se stanno chiedendo finanziamenti o se vendono token, rimangono completamente anonimi o usano pseudonimi senza una presenza pubblica verificabile, questo è un segnale di allarme. Se ci sono degli investitori dovrebbero essere in grado di identificare chi sta dietro al progetto. * Comunicazioni scarse o sospette: Se il team di sviluppo smette di comunicare con la comunità o inizia a dare risposte vaghe o sospette alle domande degli investitori, è un segno di allarme.

Ha lo stesso significato di Exit scam.

Un esempio emblematico di Rug Pull è stata la crypto Squid Game i cui anonimi creatori hanno venduto rapidamente le loro intere partecipazioni il 1° novembre 2021, portando il valore della moneta a 0.

Runes

Livello: avanzato

Argomento: tecnologia

Runes è un protocollo per la creazione di token fungibili su Bitcoin che è stato attivato il 20 aprile 2024 in concomitanza con il blocco 840000 del 4° halving.

Nasce come proposta di Casey Rodarmor, lo stesso che ha proposto la teoria degli Ordinals, come alternativa basata su UTXO allo standard BRC-20 per la creazione di token fungibili.

Runes dà priorità alla minimizzazione dell'UTXO set.
In termini semplici, questo approccio aiuta a prevenire la creazione non necessaria di UTXO, contribuendo all'efficienza complessiva della rete Bitcoin.

I saldi di Rune possono essere detenuti in UTXO che contengono qualsiasi importo di Rune. Inoltre, le Rune utilizzate in transazioni con messaggi di protocollo non validi verrebbero bruciate, consentendo a futuri aggiornamenti di cambiare il modo in cui vengono assegnate o create dai vecchi client.

Rispetto ai protocolli esistenti, questo approccio può promuovere una gestione dei token più efficiente e responsabile, riducendo così i danni. Un ruolo chiave di questo modello è quello di mantenere la verificabilità e la trasparenza di Bitcoin, risolvendo efficacemente il problema della doppia spesa.

Il protocollo utilizza la funzione OP_RETURN per archiviare i dati nelle transazioni on-chain senza la necessità modificare il protocollo Bitcoin. Questo metodo mantiene le transazioni efficienti e riduce al minimo il carico sulla rete, migliorando l'esperienza utente.

Runes è anche compatibile con Lightning Network.

In breve, Runes è un protocollo progettato per consentire la creazione e la gestione di token sulla blockchain Bitcoin in modo efficiente e responsabile. Questo viene fatto allineandosi perfettamente con l'infrastruttura di Bitcoin e minimizzando l'UTXO set.

Convenzione sui nomi delle Rune Al momento del lancio, il protocollo stabilisce che si possono usare solo nomi di rune composti da 13 a 26 caratteri. Ogni quattro mesi fino al prossimo Halving, viene sbloccato un limite di caratteri più breve, ad esempio, tutti i nomi di 12 caratteri saranno sbloccati entro agosto 2024. Ciò culminerà nello sblocco dei nomi di rune di un carattere nel 2028.

Runestone Messaggi di protocollo Rune, chiamati runestone (pietre rune), vengono memorizzati negli output delle transazioni Bitcoin.

Lo scriptPubKey di un output di runestone inizia con un OP_RETURN, seguito da OP_13 e da zero o più push di dati. Questi push di dati vengono concatenati

e decodificati in una sequenza di interi a 128 bit, per poi essere analizzati in una runestone.

Una transazione può contenere al massimo una runestone.

Una runestone può incidere (etching) una nuova Runa, coniare (mint) una Runa esistente e trasferire Rune dagli input di una transazione ai suoi output.

Un output di transazione può contenere saldi di un numero qualsiasi di Rune.

Le Rune sono identificate da ID, che consistono nel blocco in cui una Runa è stata incisa e nell'indice della transazione di incisione all'interno di quel blocco, rappresentati nel testo come BLOCCO:TX. Ad esempio, l'ID della Runa coniata nella 20esima transazione del 500esimo blocco è 500:20.

Edict Gli Edict, editti, sono un meccanismo all'interno del protocollo che consente la distribuzione o l'allocazione delle rune in una transazione Bitcoin secondo regole specifiche.

Un edict è costituito da tre componenti principali: un rune ID, un importo e un numero di output.

Pointer (Puntatore) Dopo che tutti gli editti sono stati elaborati, le rune rimanenti non allocate vengono trasferite al primo output non-OP_RETURN della transazione. Una runestone può facoltativamente contenere un puntatore che specifica un output predefinito alternativo.

Burning Le rune possono essere bruciate (burned) trasferendole su un output OP_RETURN con un editto o un puntatore.

Cenotaph Le runestone possono essere malformate per una serie di motivi, tra cui opcodice non pushdata nell'OP_RETURN della runestone, varint non validi o campi runestone non riconosciuti. Le runestone malformate sono chiamate cenotaph, cenotafi.
Le Rune fornite come input a una transazione con un cenotafio vengono bruciate.
Le Rune "incise" in una transazione con un cenotafio vengono impostate come non coniabili. I conii in una transazione con un cenotafio vengono conteggiati nel limite massimo di conio, ma le Rune coniate vengono bruciate.
I cenotafi sono un meccanismo di aggiornamento che consente di assegnare nuovi significati alle runestone, modificando il modo in cui le Rune vengono create e trasferite, senza però trarre in inganno i client non aggiornati sulla posizione di queste Rune, poiché i client non aggiornati le vedranno come bruciate.

S2F

Acronimo di: Stock-to-Flow

Livello: avanzato

Argomento: finanza

S2F, Stock-to-flow, è un modello utilizzato per valutare il valore di un bene scarso come l'oro o Bitcoin. Il modello si basa sulla relazione tra:

- **stock:** la quantità di un bene disponibile
- **flow**: e la quantità che viene prodotta ogni anno

Bitcoin ha un alto Stock-to-flow perché la sua offerta è limitata a 21 milioni di unità e la sua emissione è programmata per diminuire nel tempo attraverso l'utilizzo di un algoritmo di mining.

È una misura della nuova offerta di un'attività che viene creata nel tempo rispetto all'offerta esistente, è un numero che mostra quanti anni, all'attuale tasso di produzione, sono necessari per raggiungere lo stock attuale.

Questo rapporto può essere espresso in diversi modi, compresa la percentuale dell'offerta che viene aggiunta annualmente, o il numero di anni che l'offerta impiegherebbe per raddoppiare al tasso di produzione attuale.

Il proponente del modello S2F sostiene che maggiore è lo Stock-to-flow di un bene più alto è il suo valore intrinseco, e che Bitcoin ha un Stock-to-flow molto alto rispetto alle altre attività, e quindi è un investimento più sicuro.

Lo stock-to-flow è una metrica comunemente citata nei mercati di Bitcoin, e viene a volte utilizzato per cercare di prevederne il prezzo. Attualmente, Bitcoin ha un rapporto stock/flusso simile a quello dell'oro. Tuttavia, il rapporto di Bitcoin diminuirà continuamente nei prossimi anni, mentre quello dell'oro no.

Il modello Stock-to-Flow di PlanB è diventato popolare a marzo 2019, durante la breve bull run che ha caratterizzato il Q1 2019. È considerata una delle valutazioni quantitative principali.

È importante notare che il modello S2F non è universalmente accettato e ci sono molte critiche al suo utilizzo per valutare il valore di Bitcoin. Il prezzo di Bitcoin è influenzato da molte variabili e non dipende solo dalla sua offerta limitata.

Il rapporto stock-to-flow di Bitcoin è molto più prevedibile e precisamente verificabile in qualsiasi momento. Lo stock-to-flow di Bitcoin continuerà a diminuire indefinitamente man mano che l'offerta aumenta e l'halving di Bitcoin riduce il tasso di produzione in modo graduale ogni quattro anni.

SAFT

Acronimo di: Simple Agreement for Future Tokens

Livello: avanzato

Argomento: finanza

Un SAFT un accordo di vendita di tokens contenente un diritto a future unità di token acquistate dagli investitori a un prezzo scontato ai fini del finanziamento e dello sviluppo di un progetto crypto, che garantisce che il prezzo del token sia stabilito in anticipo e che il token non verrà rilasciato fino a quando il progetto non avrà raggiunto una certa milestones.

sat

Acronimo di: Satoshi

Livello: base

Argomento: tecnologia

Il satoshi, a volte abbreviato in Sat, è la più piccola unità di misura del bitcoin, la criptovaluta creata da Satoshi Nakamoto nel 2009. Un satoshi è equivalente a 1/100 milionesimo di bitcoin, o 0,00000001 BTC.

Il nome è stato scelto in onore dell'enigmatico creatore del Bitcoin, noto come Satoshi Nakamoto.

Nonostante il satoshi sia l'unità di misura più piccola sulla blockchain di Bitcoin, sulla rete Lightning Network è possibile frazionarlo ulteriormente fino al millesimo di satoshi. Questa suddivisione ulteriore consente transazioni più precise e micro-pagamenti su questa rete di secondo livello.

Prima dell'introduzione del termine Sats, per il frazionamento di Bitcoin veniva utilizzato il termine Bit, che corrisponde al milionesimo di bitcoin. Quindi 1 bit corrisponde a 100 Sat.

Satoshi Nakamoto

Livello: base

Argomento: tecnologia

È il nome utilizzato dalla presunta persona o dalle persone pseudonime che hanno sviluppato Bitcoin, hanno scritto il white paper Bitcoin, creato e distribuito l'implementazione di riferimento originale di bitcoin.

L'11 febbraio 2009, Satoshi Nakamoto scrisse di una prima versione di Bitcoin su un forum online per cypherpunk, persone che lavorano sulla tecnologia di crittografia e si preoccupano della privacy e della libertà individuale. Sebbene questo non sia il primo annuncio ufficiale del rilascio di Bitcoin, contiene un buon riassunto delle motivazioni di Satoshi.

Scalability

Scalabilità

Livello: intermedio

Argomento: tecnologia

è la capacità di un sistema informatico di poter adeguare le proprie capacità per continuare a funzionare correttamente in presenza di un maggior carico. Il problema della scalabilità dei bitcoin, a causa del limite della dimensione del blocco della blockchain, è un argomento ampiamente dibattuto con proposte che hanno portato anche alla scissione della comunità e relativi fork

Scalping

Livello: avanzato

Argomento: finanza

È un modo strategico di fare trading, in quanto riguarda la tecnica di fare compravendite veloci, a breve termine. Il termine può riferirsi a tutti gli asset su cui investire nel trading online e non solo alle criptovalute.

Lo scalping è uno stile di trading specializzato nel trarre profitto da piccole variazioni di prezzo e ottenere un rapido profitto dalla rivendita. Nel day trading, scalping è un termine per una strategia che dà la priorità alla realizzazione di volumi elevati con piccoli profitti. Lo scalping richiede che un trader abbia una strategia di uscita rigorosa perché una grande perdita potrebbe eliminare i tanti piccoli guadagni per cui il trader ha lavorato. Pertanto, affinché questa strategia abbia successo, è necessario disporre degli strumenti giusti, come un feed live, un broker ad accesso diretto e la resistenza per effettuare molte operazioni.

Avere gli strumenti giusti, come un feed live, un broker ad accesso diretto e la resistenza per effettuare molte operazioni, è necessario affinché questa strategia abbia successo. Uno scalper di azioni di successo avrà un rapporto molto più alto di operazioni vincenti rispetto a quelle perse, mantenendo i profitti più o meno uguali o leggermente maggiori delle perdite. Uno scalper puro farà un certo numero di operazioni ogni giorno, forse centinaia.

Scam/Scammer

Truffa/truffatori

Livello: base

Argomento: finanza

Con questo termine ci si riferisce a truffe/truffatori e altre attività illecite: è un termine applicabile a tutti i tipi di circonvenzione.

Schelling point

Livello: intermedio

Argomento: politica

Lo Schelling point, anche noto come punto di Schelling o punto focale di Schelling, concetto utilizzato nella teoria dei giochi, è una soluzione che i giocatori tendono ad adottare in assenza di comunicazione, poiché esso appare naturale, speciale o rilevante per loro.

Nella teoria della coordinazione è usata per descrivere una soluzione che emerge in maniera naturale da una situazione di coordinamento senza alcuna comunicazione esplicita tra i partecipanti.

I punti di Schelling possono essere utili per risolvere i giochi in cui i giocatori non possono comunicare tra loro. Possono anche essere utili per creare una coesione sociale e un senso di comunità.

Il nome del concetto deriva dal nome del premio Nobel Thomas C. Schelling, uno degli economisti che ha contribuito a svilupparlo e a studiarlo nel suo libro del 1960 The Strategy of Conflict.

Immagina una situazione in cui due o più persone devono prendere una decisione su un determinato aspetto, ma non possono comunicare direttamente tra loro. In queste situazioni, le persone tendono a convergere spontaneamente verso una soluzione che sembra naturale o ovvia, anche se non ci sono incentivi o regole esterne a guidarli in quella direzione.

Il punto di Schelling è quindi quel risultato o soluzione che appare come il punto di incontro più "naturale" o "ovvio" in una situazione data, a causa di fattori psicologici, sociali o culturali. Può essere considerato un punto di convergenza implicito o una convenzione emergente, dove le persone si aspettano che gli altri partecipanti scelgano la stessa opzione.

Un classico esempio del punto di Schelling è il "gioco delle coordinate." Immaginiamo che due persone debbano incontrarsi in una città sconosciuta, ma non possono comunicare tra loro. Ognuno può scegliere un punto sulla mappa come punto di incontro, e il punto di Schelling in questa situazione sarebbe probabilmente un luogo facilmente riconoscibile o noto, come un monumento famoso o una piazza centrale.

In sintesi, lo Schelling point rappresenta una soluzione di coordinamento spontanea che emerge in assenza di comunicazione diretta, basata su considerazioni di ovvietà, convenzione o familiarità.

L'oro è uno Schelling point. Sono state le sue elementali del metallo giallo che hanno fatto sì che il mondo intero convergesse sull'oro come la soluzione più efficiente in termini di denaro disponibile: portabile, divisibile, scarso, non arrugginisce, non corrode, e così via.

Nessuno ha dovuto comunicare per determinare che l'oro era il materiale migliore per il lavoro, tutti gli altri elementi sono stati eliminati da un processo di ragionamento o esperimento.

Bitcoin è il primo asset a offrire alternativa digitale all'oro.

Bitcoin ha il potenziale per diventare Schelling point: ha un'ampia base di utenti, è scarso e la sua emissione non può essere controllata da alcuna autorità centrale. Bitcoin è una soluzione digitale all'inflazione e alla svalutazione monetaria, problemi che stanno diventando sempre più importanti nel mondo moderno.

Schnorr signatures

Livello: avanzato

Argomento: tecnologia

Le Schnorr signatures, o firme di Schnorr, sono un modo potente per autenticare le transazioni Bitcoin, che sono state introdotte nel protocollo Bitcoin attraverso il soft fork Taproot.

Sono firme digitali che forniscono una sicurezza simile allo schema ECDSA utilizzato dall'implementazione originale di Bitcoin e che possono utilizzare gli stessi parametri della curva ellittica di Bitcoin, ma che possono fornire altri vantaggi.

I presupposti di sicurezza Schnorr sono analoghi a quelli di ECDSA ed è più facile e veloce creare firme multiparte sicure utilizzando Schnorr con protocolli come MuSig.

Lo schema Schnorr presenta diversi vantaggi rispetto all'ECDSA ed è quindi attualmente in fase di implementazione in Bitcoin tramite l'aggiornamento Taproot.

In primo luogo, lo schema Schnorr è sicuramente sicuro e non malleabile ovvero non soffre del problema noto come Transaction Malleability, due miglioramenti rispetto all'ECDSA.

In secondo luogo, rispetto alle firme ECDSA, le firme Schnorr richiedono meno tempo per essere verificate. Le firme Schnorr e le chiavi pubbliche possono essere aggregate, il che significa che più parti con chiavi private univoche possono firmare lo stesso messaggio con un'efficienza molto maggiore.

Grazie a questa funzione, le firme Schnorr possono essere verificate in batch anziché singolarmente, velocizzando ulteriormente la verifica. L'aggregazione di chiavi e firme consente anche guadagni in termini di privacy oscurando il numero di firme presenti su una transazione.

Infine, le firme Schnorr sono anche più piccole delle firme ECDSA, offrendo risparmi sulle commissioni per coloro che spendono i prodotti Schnorr.

Quando è stato inventato Bitcoin, lo schema Schnorr era ancora protetto da brevetto, e quindi Satoshi Nakamoto ha deciso di utilizzare ECDSA come schema di firma per Bitcoin. Da allora il brevetto Schnorr è scaduto e quindi sono liberamente utilizzabili.

Script

Livello: avanzato

Argomento: tecnologia

Lo Script è un elemento fondamentale per i Bitcoin, perché le transazioni Bitcoin non sono soltanto dei trasferimenti di valore da un wallet ad un altro, ma sono dei programmi più o meno semplici, definiti anche smart contract, in un linguaggio di scripting che stabiliscono come i Bitcoin possono essere trasferiti o spesi.

Questi smart contract Bitcoin di base consentono di definire le regole come bloccare e sbloccare i fondi. Tuttavia, Bitcoin Script, come linguaggio di programmazione, è abbastanza limitato alla logica di base che entra in gioco solo quando si spostano le monete in una nuova transazione.

Ad esempio la prima forma di pagamento Bitcoin, chiamata P2PK Pay-to-Public-Key in italiano Paga alla Chiave pubblica (ormai obsoleta) è realizzata con uno script di poche istruzioni.

Il linguaggio di scripting di Bitcoin si chiama semplicemente Script. Tutti gli script Bitcoin sono scritti in Script.

Satoshi Nakamoto lo definisce in questo modo:
"*Lo script è in realtà un predicato. È solo un'equazione che si valuta come vera o falsa. Predicato è una parola lunga e poco familiare, quindi l'ho chiamata script.*"

Bitcoin Script è un linguaggio simile al Forth basato su stack. È un linguaggio che generalmente viene considerato non Turing complete, perché volutamente manca di diverse funzioni logiche, inclusi i loop. Questo viene fatto per garantire che nessuno script Bitcoin possa consumare una potenza di calcolo eccessiva e danneggiare i nodi della rete.

Lo script viene utilizzato quasi esclusivamente per le transazioni, e possiamo classificare in 2 categorie gli script:

- script di blocco, o output script, storicamente chiamato scriptPubKey
- script di sblocco, o input script, storicamente chiamato scriptSig

Una transazione è composta da un insieme di input UTXO in ingresso, ognuno dei quali ha il suo scriptPubKey che definisce come l'UTXO può essere speso o trasferito, e questo trasferimento viene sbloccato nella transazione tramite lo scriptSig. Lo script bitcoin serve quindi principalmente per bloccare e sbloccare bitcoin, non per creare applicazioni o eseguire programmi generici. La semplicità di Script offre anche sicurezza a Bitcoin e rende più facile per gli sviluppatori evitare di perdere denaro durante la progettazione di portafogli o applicazioni su Bitcoin. Questi script vengono a volte chiamati smart contract.

Tutte le transazioni Bitcoin utilizzano Script per definire come possono essere spesi gli output. In altre parole, lo script di una transazione Bitcoin determina

a chi è stato inviato il bitcoin. Bitcoin ha alcuni script diversi, con Pay-to-Public-Key-Hash (P2PKH) che è il più popolare. P2PKH è un semplice script che paga bitcoin a un indirizzo, indicato attraverso il suo hash. Altri script possono ottenere configurazioni più complesse, come la creazione di indirizzi multisig. Per spendere i Bitcoin inviati ad un indirizzo multisig viene richiesto più firme da più chiavi private. Sebbene i tipi di script SegWit, P2WPKH e P2WSH, offrano risparmi sulle commissioni di transazione, l'adozione di questi nuovi tipi di script è volutamente lenta. Ad aprile 2021, quasi quattro anni dopo l'attivazione di SegWit, gli script P2PKH sono utilizzati da oltre il 70% degli UTXO.

Gli script sono composti da opcode, i comandi di base, con i dati aggiuntivi come indirizzi, chiavi pubbliche e firme.

script path

Livello: avanzato

Argomento: tecnologia

Tapscript è il linguaggio di scripting usato per gli script-path di taproot.

Script Type Heuristic

Livello: avanzato

Argomento: legale

La Script Type Heuristic, o euristica del tipo di script, è un metodo utilizzato per la Chain Analysis e dedurre informazioni sugli indirizzi coinvolti.

In Bitcoin, ogni transazione spende delle entrate che sono legate ad un determinato script di output. Questi script possono essere di diversi tipi, come P2PKH (Pay-to-Public-Key-Hash) o P2SH (Pay-to-Script-Hash), e ciascuno di questi ha un determinato formato e una serie di regole per la loro validazione.

L'euristica del tipo di script si basa sull'ipotesi che gli indirizzi utilizzati per ricevere fondi in un determinato tipo di script siano utilizzati per scopi specifici. Ad esempio, gli indirizzi P2PKH sono spesso utilizzati per ricevere fondi da wallet personali mentre gli indirizzi P2SH sono spesso utilizzati per ricevere fondi da servizi di multisignature o script complessi.

Ad esempio, se un utente riceve un pagamento a un indirizzo P2PKH e poi spende questo output per creare due output, una a un indirizzo P2SH e una a un indirizzo P2PKH, si può ipotizzare che l'output P2SH appartenga a una terza parte, mentre l'output P2PKH è un'output di resto e appartiene ancora al mittente.

La script Type Heuristic è un metodo comunemente utilizzato nell'chain analysis per identificare gli indirizzi coinvolti in una transazione e per ricostruire le

relazioni tra indirizzi. Tuttavia, questo metodo può essere ingannato da tecniche di privacy come Coinjoin o Payjoin, in cui più indirizzi condividono la stessa entrata e quindi lo stesso tipo di script.

Come tutte le euristiche di chain analysis, si tratta di un'ipotesi e non ha alcuna certezza. Inoltre, l'aggiornamento di Taproot e i futuri aggiornamenti del protocollo Bitcoin potrebbero rendere questa euristica inutile, poiché i tipi di transazione diventano meno distinguibili.

scriptless multisignature

Livello: avanzato

Argomento: tecnologia

Le scriptless multisignature, o multifirme senza script rendono possibile che un numero essenzialmente illimitato di persone crei una singola chiave pubblica che può essere spesa con una singola firma da parte di tutti loro, aumentando notevolmente la scalabilità e la privacy di Bitcoin.

Le scriptless multisignature sono firme digitali create utilizzando due o più chiavi private che possono essere verificate utilizzando solo una singola chiave pubblica e una singola firma.

È possibile creare multifirme per l'algoritmo ECDSA supportato da tutte le versioni di Bitcoin, anche se le firme di Schnorr rendono le scriptless multisignature molto facili e sono noti diversi algoritmi per questo scopo, con MuSig che è stato creato specificamente per le esigenze degli utenti di Bitcoin.

Le scriptless multisignature possono essere paragonate alle multifirme con script, che utilizzano chiavi pubbliche e firme con gli opcode OP_CHECKMULTISIG e OP_CHECKMULTISIGVERIFY di Bitcoin (e l'opcode OP_CHECKSIGADD proposto per Tapscript).
Le multifirme hanno il vantaggio che solo una singola chiave e una singola firma vengono pubblicate onchain quando vengono utilizzate in una transazione Bitcoin, consentendo a un numero illimitato di firmatari di pagare lo stesso importo di commissione di transazione che un singolo firmatario pagherebbe per una transazione altrimenti identica. Il fatto che i pagamenti multifirma siano indistinguibili dai pagamenti a firma singola offre inoltre una maggiore privacy ai creatori di entrambi i tipi di pagamenti.

ScriptPubKey

Livello: avanzato

Argomento: tecnologia

I bitcoin non si trovano all'interno di un wallet, ma sono degli importi non spesi registrati nella blockchain chiamati UTXO.

Questi UTXO contengono una informazione chiamata **ScriptPubKey**, conosciuta anche come locking script, che stabilisce quali sono le regole per poter spendere o trasferire l'importo indicato nell'UTXO. Lo ScriptPubKey è lo script nell'UTXO che imposta le condizioni per spendere (trasferire) i bitcoin dell'UTXO.

Uno ScriptPubKey viene spesso chiamato locking script perché blocca (lock) i bitcoin finché qualcuno non può fornire una risposta (o soluzione dello script) per sbloccarli e quindi trasferirli attraverso uno ScriptSig o unlocking script.

Ci sono diversi tipi di ScriptPubKey.

- P2PK: il primo, il più semplice, ma ormai obsoleto, è P2PK, Pay-to-Public-Key, paga alla chiave pubblica che è inserita in chiaro nello script. Per spendere i bitcoin bloccati con P2PK, si deve produrre una firma con la chiave privata corrispondente alla chiave pubblica inserita nello script.
- P2PKH: il primo script P2PK è stato presto sostituito da P2PKH, Pay-to-Public-Key-Hash, che sostituisce la chiave pubblica in chiaro con l'hash della chiave pubblica, aggiungendo sicurezza e privacy.

A questi primi tipi di script se ne sono aggiunti altri nel tempo:

- nel 2013 P2SH Pay-to-Script-Hash
- nel 2017, con l'aggiornamento SegWit, P2WPKH e P2WSH
- nel 2021, con l'aggiornamento Taproot, P2TR Pay-to-Taproot

Questa *risposta* che consente di sbloccare i bitcoin, avviene tramite lo script di sblocco, unlocking script, chiamato ScriptSig nelle transazioni legacy e Script Witness nelle transazioni SegWit, e viene fornito quando questo bitcoin viene speso tramite una transazione.

ScriptSig

Livello: intermedio

Argomento: tecnologia

Lo ScriptSig, più precisamente definito come unlocking script, è la parte di una transazione che contiene le firme richieste e lo script che sblocca un UTXO per poter essere speso.

Uno ScriptSig si combina con lo ScriptPubKey per formare uno script completo e valido.

Lo ScriptSig è presente solo nelle transazioni Bitcoin legacy, ovvero quelle con il vecchio formato.

Nelle transazioni SegWit, lo ScriptSig viene rimosso dal corpo della transazione e viene chiamato Witness Script.

Quando viene inviato bitcoin, viene bloccato utilizzando una ScriptPubKey.

Lo ScriptPubKey può essere pensato come un indovinello, risolvibile solo dal proprietario delle chiavi private corrette. Per spendere questo bitcoin, il proprietario deve pubblicare la risposta all'enigma firmando la transazione con le sue chiavi.

La risposta pubblicata all'indovinello è ScriptSig.

Ogni nodo verifica che ScriptSig corrisponda allo ScriptPubKey per ogni transazione ricevuta, assicurando che nessuna transazione non valida venga aggiunta alla blockchain. Uno dei principali cambiamenti implementati in SegWit è stato il trasferimento di ScriptSig dal corpo della transazione legacy alla parte Witness.

ScriptSpend

Livello: avanzato

Argomento: tecnologia

Lo ScriptSpend e lo script di spesa.

Nel caso di Taproot gli output (UTXO) si possono spendere in due modi: KeySpend e ScriptSpend. Con KeySpend si deve fornire la chiave, o meglio una firma bip-schnorr per la chiave pubblica nell'output, mentre con ScriptSpend non viene utilizzata una chiave ma uno script.

Contrariamente ai precedenti formati delle transazioni Bitcoin, l'output di Taproot non distingue tra un public KeySpend path e uno ScriptSpend path.

Lo ScriptSpend path è un modo alternativo al public key path per spendere l'output di P2TR, e può essere utilizzato come caso di ripiego quando la spesa collaborativa è impossibile. Un singolo script o molti script organizzati nel Merkle tree possono essere utilizzati per coprire molti scenari diversi.

Scrypt

Livello: intermedio

Argomento: tecnologia

Un algoritmo Proof-of Work (PoW) alternativo a SHA-256, ovvero quello utilizzato nel mining Bitcoin: Scrypt si basa più sulla memoria che sulla pura potenza della CPU, con l'obiettivo di ridurre il vantaggio che gli ASIC hanno e quindi aumentare la partecipazione della rete e l'efficienza energetica. Utilizzato ad esempio da Litecoin.

SDN List

Acronimo di: Specially Designated Nationals and Blocked Persons List

Elenco dei cittadini specialmente designati e delle persone bloccate

Livello: intermedio

Argomento: legale

Una SDN List, acronimo di Specially Designated Nationals and Blocked Persons List, Elenco dei cittadini specialmente designati e delle persone bloccate, è un elenco compilato dall'OFAC che identifica individui e società soggetti a sanzioni statunitensi.
Queste sanzioni sono progettate per impedire a persone e organizzazioni designate di accedere al sistema finanziario degli Stati Uniti e di impegnarsi in attività che potrebbero compromettere la sicurezza nazionale degli Stati Uniti.

Gli indirizzi Bitcoin sono trattati come qualsiasi altro tipo di proprietà bloccata nell'ambito delle sanzioni statunitensi. Ciò significa che è illegale per gli statunitensi o le persone o entità presenti negli Stati Uniti di effettuare transazioni con indirizzi Bitcoin elencati nella SDN List.

Quando un indirizzo Bitcoin viene aggiunto alla SDN List, l'OFAC fornisce un identificatore alfanumerico univoco per l'indirizzo e specifica la valuta digitale a cui corrisponde l'indirizzo. Ad esempio, un indirizzo Bitcoin elencato nella SDN List potrebbe apparire come "Digital Currency Address - XBT: 123456789abcdef".

SEC

Acronimo di: Securities and Exchange Commission

Commissione per i Titoli e gli Scambi

Livello: base

Argomento: politica

La SEC (Securities and Exchange Commission) è l'agenzia indipendente del governo federale degli Stati Uniti responsabile dell'applicazione delle leggi federali sulle Security, i titoli, propone norme sui titoli e regola il mercato degli asset, gli scambi azionari e altre attività e organizzazioni correlate.

Finora, la SEC non ha ritenuto che Bitcoin stesso sia una Security, ma ha preso posizioni diverse nei confronti di diverse offerte di criptovalute e ICO.
La SEC ha affermato che alcune offerte di token possono essere considerate come Security, soggette alle relative leggi federali.

A giugno 2022 Gary Gensler, allora presidente della SEC, parlando di criptovalute ha definito Bitcoin come commodity: "*Alcune, come Bitcoin, e questo è l'unica che posso dire… sono commodities*"

di fatto escludendo che Bitcoin possa essere considerato security, ma ipotizzando che in linea di massima tutte le altre possano esserlo:

"*Dei circa 10.000 token presenti sul mercato delle criptovalute la stragrande maggioranza è costituita da security. Le offerte e le vendite di queste migliaia di security token sono coperte dalle leggi sulle security. Alcuni token potrebbero non soddisfare la definizione di security - quelli che chiamerò crypto non-security token. Questi rappresentano probabilmente solo un piccolo numero di token, anche se possono rappresentare una parte significativa del valore aggregato del mercato delle criptovalute.*"

Ciò significa che le persone o le aziende che desiderano effettuare un'offerta di token che può essere considerata un titolo devono conformarsi alle leggi sulla sicurezza e ottenere l'approvazione della SEC, a meno che non esistano esenzioni specifiche.

La SEC ha anche emesso avvisi agli investitori sui rischi delle criptovalute e ha preso provvedimenti legali contro diverse aziende e individui che, secondo l'ente, hanno violato le leggi sulle Security nell'ambito delle offerte di criptovalute.

Secondo alcuni economisti le imprevedibili azioni di applicazione della SEC nel periodo sotto la presidenza di Gary Gensler, dal 2021 al 2025, classificando le criptovalute come titoli senza linee guida chiare, hanno causato una prolungata destabilizzazione nei mercati delle criptovalute.
Le linee guida poco chiare sollevano dubbi sulla capacità dell'agenzia di mantenere mercati equi e ordinati.

Ha febbraio 2025 la SEC ha dichiarato che la maggior parte delle meme coin non soddisfa la definizione di titoli ai sensi della legge federale, esentandole dai requisiti di registrazione.

SEC Format

Livello: avanzato

Argomento: tecnologia

Il Formato SEC, Standards for Efficient Cryptography, è un metodo standard per codificare una chiave pubblica Bitcoin.

Una chiave pubblica Bitcoin è un punto sulla curva ellittica, chiamato secp256k1, e quindi ha una coordinata x e una y. Tuttavia, ogni valore x ha solo due possibili valori y e, a causa della natura di secp256k1, uno di questi valori y è dispari e l'altro è pari per ogni valore x. Pertanto, il valore x e la parità del valore y sono sufficienti per identificare la chiave pubblica. La parità del valore y viene visualizzata da un byte 0x02 o 0x03, che indicano rispettivamente pari o dispari. Questo è seguito dal valore x, che è un numero di 32 byte.

Questo formato è chiamato compresso, perché occupa solo 33 byte, rispetto al formato SEC non compresso, che inizia con un prefisso 0x04 seguito dai valori x e y completi e occupa 65 byte.

Second-Layer Solutions

Livello: intermedio

Argomento: tecnologia

Le Soluzioni second layer o Layer 2, in italiano “di secondo livello”, sono un insieme di soluzioni basate su una blockchain pubblica per estendere la scalabilità e l’efficienza, in particolare per le micro-transazioni o le azioni.

Nel caso di Bitcoin, la più conosciuta è Lightning Network.

Secp256k1

Livello: avanzato

Argomento: tecnologia

Secp256k1 è il nome della curva ellittica utilizzata da Bitcoin per implementare la sua crittografia a chiave pubblica.

Tutti i punti su questa curva sono chiavi pubbliche Bitcoin valide.

Quando un utente desidera generare una chiave pubblica utilizzando la propria chiave privata, moltiplica la propria chiave privata, un numero molto grande, per il Generator Point, un punto definito sulla curva secp256k1.

Grazie al Discrete Log Problem, la divisione di una chiave pubblica per il Generator Point non può produrre una chiave privata.

Tutte le curve ellittiche sono equazioni con un modello specifico: y^2 = x^3 ax^ b. Per secp256k1 in particolare, a = 0 e b = 7, ottenendo l’equazione y^2 = x^3 7. Poiché la componente y dell’equazione è al quadrato, secp256k1 è simmetrico rispetto all’asse x e per ogni valore di x, ci sono due valori di y, uno dei quali è dispari mentre l’altro è pari.

Ciò consente di identificare le chiavi pubbliche semplicemente dalla coordinata x e dalla parità della coordinata y, risparmiando un utilizzo significativo dei dati sulla blockchain.

Secure Element

Livello: intermedio

Argomento: tecnologia

Il secure element di un hardware wallet è un componente hardware critico che fornisce un ambiente sicuro e isolato per eseguire operazioni di crittografia e memorizzare in modo sicuro le chiavi private utilizzate per l’accesso alle criptovalute.

Il secure element è un chip specializzato con funzionalità avanzate di sicurezza, progettato per resistere ad attacchi fisici e logici.

È progettato per essere resistente a manipolazioni esterne, come tentativi di rimozione del chip o analisi del suo contenuto. Inoltre, è in grado di rilevare e resistere a tentativi di attacchi logici, come l'intercettazione dei dati durante la comunicazione con il dispositivo.

L'utilizzo di un secure element fornisce un livello di protezione aggiuntivo rispetto ad altre forme di archiviazione delle chiavi private, come i wallet software eseguiti su computer o smartphone. Poiché il chip è isolato dal sistema operativo dell'host e da altre applicazioni, le chiavi private non possono essere compromesse da malware o altre minacce che potrebbero essere presenti sul dispositivo.

Gli hardware wallet che utilizzano un secure element offrono quindi un elevato livello di sicurezza per la gestione delle chiavi private delle criptovalute. Consentono agli utenti di generare, archiviare e firmare transazioni in modo sicuro, offrendo una soluzione affidabile per la gestione dei propri asset digitali.

Il Secure Element serve per evitare o ridurre la probabilità di estrazione da parte di un avversario, nonché (in alcuni casi) per eseguire determinate operazioni internamente al chip stesso al fine di limitare la quantità di informazioni segrete che vengono gestite al di fuori del Secure Element (in memorie meno sicure).

Il Secure Element protegge il segreto (seed o chiave privata) fino a quando l'utente non sblocca l'accesso, ad esempio inserendo il PIN; una volta fatto ciò, i dati diventano leggibili.

Ci sono diversi hardware wallet (che utilizzano anche il Secure Element) che consentono di visualizzare il mnemonic memorizzato nel dispositivo una volta autorizzata dall'utente.

Security

Livello: intermedio

Argomento: finanza

Nel settore Bitcoin e cripto, il termini Commodity e Security vengono utilizzati spesso in contrapposizione per definire una criptovaluta. In questo contesto, generalmente viene utilizzato il seguente significato:

- **Commodity**: bene tangibile, il cui valore sottostante è dato dall'utilità percepita come mezzo di pagamento, riserva di valore o strumento di investimento.
- **Security**: titolo che rappresenta una partecipazione o un credito nei confronti di una organizzazione o una società, il cui valore sottostante è dato dall'utilità percepita di quell'organizzazione o società.

Si sta affermando la posizione secondo la quale Bitcoin sia una commodity, e tutte le altre cripto security.

Nel contesto finanziario una security è un contratto di investimento, che crea un dovere fiduciario. Nel caso delle criptovalute, una cripto, coin o token, potrebbero essere definiti come security quando possiedono le caratteristiche di "titolo" collegato all'attività finanziaria. In tal caso, possiamo definire il token come "security token".

Per Security si intende uno strumento finanziario fungibile e negoziabile che rappresenta una forma di valore sottostante.
Concettualmente, una security implica un investimento e un'aspettativa di profitto. Molti token sono considerati security nell'economia digitale, anche se potrebbero non possedere tutti gli elementi convenzionali di una security. La forma più pura di security include azioni, obbligazioni, merci o derivati negoziabili.

Tuttavia, la classificazione di un token come security può variare a seconda della giurisdizione, poiché le diverse regioni utilizzano diverse classificazioni legali per determinare cosa costituisce un titolo. In generale, i titoli sono classificati in azioni, debiti o una combinazione dei due. Quando si definisce un token e le sue caratteristiche, si cerca di determinare se il token può essere considerato una security. In tal caso, potrebbe essere soggetto alle normative sulla sicurezza e richiedere adempimenti significativi.

Negli Stati Uniti, le autorità di riferimento per le security sono la Securities and Exchange Commission (SEC) e la Financial Industry Regulatory Authority (FINRA). Entrambe le autorità stanno sempre più intervenendo nel settore delle criptovalute, ma l'applicazione delle vecchie normative a un settore così innovativo come quello delle criptovalute può essere controversa. Inoltre, il carattere globale delle criptovalute rende difficile l'applicazione di regolamentazioni in una singola giurisdizione.

Nel giugno 2022 Gary Gensler, presidente della SEC, ha definito Bitcoin come una commodity escludendo che possa essere considerato una security. Tuttavia, ha suggerito che la maggior parte delle altre criptovalute potrebbero essere considerate security. Sempre Gensler, a giugno 2023 nelle azioni esecutive contro Binance e Coinbase ha esplicitamente elencato diverse criptovalute indicandole come security.

Sul tema della globalizzazione delle criptovalute e sulla loro giurisdizione, a settembre 2022 la SEC nell'intentare causa federale contro l'influencer di criptovalute Ian Balina per la mancata registrazione di una criptovaluta come security prima del lancio di un'offerta iniziale di monete (ICO) nel 2018, ha evidenziato che gli ETH sono *"convalidati da una rete di nodi sulla blockchain di Ethereum, che sono raggruppati più densamente negli Stati Uniti che in qualsiasi altro paese"*, concludendo quindi che: *"Di conseguenza, tali transazioni hanno avuto luogo negli Stati Uniti"*, una interpretazione a dir poco azzardata, ma in linea con l'atteggiamento delle agenzie di controllo statunitensi.

La determinazione se un titolo o un token è una security secondo la giurisdizione statunitense, e in modo esteso anche ad altre giurisdizioni, talvolta fa riferimento

al Howey test, che si riferisce a una causa della SEC.

Un security token dovrebbe rappresentare una promessa di una quota di profitti o guadagni futuri, simile ai titoli scambiati sui mercati azionari o obbligazionari.

I security token rappresentano una quota tokenizzata nella proprietà di risorse di valore, come aziende o immobili, che viene registrata su un registro blockchain. Possono essere paragonati alle azioni societarie o alle frazioni/multipli di azioni, poiché rappresentano una partecipazione azionaria in una società. Inoltre, possono comportare una proprietà parziale di tale attività e potenziali rendimenti futuri, come il pagamento di dividendi.
Di conseguenza, i security token offrono un modo più flessibile e sicuro per trasferire, scambiare e archiviare valore.

Nell'Unione Europea, l'Autorità indipendente sulle Securities o strumenti finanziari e dei mercati è l'ESMA, e il regolamento di riferimento europeo nei mercati delle criptovalute, il MiCA.
Il MiCA non utilizza esplicitamente il termine "security" per classificare le criptovalute, ma le suddivide in ARTs (asset-referenced tokens) o token riferiti a beni, e EMTs o (e-money tokens) o token di moneta elettronica.

La Securitization è un modo per impacchettare il cash flow da asset, comprese le obbligazioni, e venderle agli investitori. Consente ai detentori di asset di accedere alla liquidità e agli investitori di accedere al valore. Si tratta di un processo mediante il quale vengono creati titoli tradizionali. La securitization è anche rilevante per alcuni casi d'uso dei security token e per i processi più avanzati di finanziamento degli asset digitali che emergono negli spazi NFT e DeFi. La securitization offre opportunità agli investitori e libera capitale per gli originator, cioè le società che detengono gli asset, favorendo la liquidità del mercato.

I security token hanno effetti simili alla securitization tradizionale, consentendo ai proprietari di asset illiquidi di accedere ai propri investimenti. Tuttavia, di solito vengono utilizzati per frazionare il valore di un'attività di alto valore anziché aggregare il valore di diverse attività di basso valore.

Security budget

Livello: avanzato

Argomento: politica

Con Security budget si intende la capacità della quantità di denaro che viene destinata alla sicurezza della rete Bitcoin attraverso la ricompensa, il Block Reward, di garantire la sicurezza stessa.

In linea teorica, più alto è il Security budget, maggiori sono le garanzie che la rete sia sicura da attacchi quali il 51% Attack.

Questo denaro viene utilizzato per compensare i miner che contribuiscono alla

sicurezza della rete mediante la creazione di nuovi blocchi e la conferma delle transazioni.

Il Block Reward è composto da:

- Block Subsidy: la quantità di nuovi bitcoin coniati in ogni blocco, che vengono assegnati al miner;
- Fee sulle transazioni: le commissioni che vengono pagate da chi effettua le transazioni.

Generalmente il Block Subsidy ha costituito la maggior parte dei ricavi del Block Reward, questo valore è fisso per ogni blocco ma ogni circa 4 anni si dimezza con quello che viene chiamato Halving.

Le fee sono variabili e ogni utente decide l'importo delle commissioni quando crea la transazione.

Il Security budget è influenzato da un lato dal Block Subsidy e dalle fee, ma anche dai costi dei miner e quindi dalla difficoltà, dal prezzo dei bitcoin.

Esiste una discussione in corso sulla possibilità che l'halving potrebbe portare ad una diminuzione dei ricavi per i miner tale da creare problemi al security budget già negli anni 2030. Il timore è che la quota parte delle fee di transazione non crescerà abbastanza da compensare la diminuzione del Block Subsidy, con una conseguente diminuzione della sicurezza della rete Bitcoin e un aumento della probabilità di attacchi, dato che i miner non sono più incentivati a partecipare.

Questa preoccupazione è stata in particolare enfatizzata da chi propone il Proof-of-Stake quale alternativa al Proof-of-Work.

Ci sono diverse controargomentazioni rispetto a questo rischio.

L'halving riduce solo la quantità di nuovi Bitcoin che vengono creati e distribuiti ai miner come ricompensa per la loro attività di mining. In realtà, l'effetto dell'halving sulla sicurezza della rete dipende dalla relazione tra il prezzo del Bitcoin e l'energia e i costi necessari per eseguire il mining. Se il prezzo del Bitcoin aumenta, ciò può compensare la riduzione della ricompensa per il mining e quindi non influire sulla sicurezza della rete.

Con l'aumento dell'adozione e dei casi d'uso, aumenta la concorrenza per aggiungere transazioni allo scarso spazio dei blocchi di Bitcoin, con un conseguente aumento delle commissioni attuali e un'ulteriore domanda di soluzioni di scaling.
Il mercato continuerà a presentare queste soluzioni di scalabilità in base alle esigenze: tra le soluzioni più diffuse vi sono gli exchanges che raggruppano le transazioni, Lightning Network e altri sviluppi di livello 2 e 3 che possono raggruppare migliaia di trasferimenti di Bitcoin in un'unica transazione che viene regolata on-chain.

La prima volta nella quale nel Block Reward le fee hanno superato il Block Subsidy è stato a maggio 2023, con il blocco 788695: 6,701 bitcoin di fee contro

i 6,25 bitcoin del Block Subsidy.

Seed

seme

Livello: base

Argomento: tecnologia

Un seed, tradotto letteralmente come *seme*, è un dato che può essere utilizzato per generare un Wallet HD. Può essere sufficiente per rigenerare le chiavi private e pubbliche del wallet, quindi è efficace come backup. Poiché il seed è deterministico, un dato seed genererà sempre le stesse chiavi e un singolo seed può generare un numero quasi infinito di chiavi pubbliche e private.

In sostanza un seed è una stringa casuale di cifre.

Un seed viene utilizzato per generare una singola chiave privata estesa (xprv), chiamata chiave privata master. Questa chiave privata può essere utilizzata per generare chiavi private secondarie e chiavi pubbliche, consentendo a un wallet di generare tutte le coppie di chiavi necessarie all'utente. Questa configurazione massimizza la facilità di backup di un wallet con i vantaggi per la privacy di evitare il riutilizzo degli indirizzi.

I seed sono spesso rappresentati come frasi mnemoniche per rendere semplice memorizzarle. I seed sono diventati uno standard della comunità grazie al BIP32, mentre le frasi mnemoniche sono diventate uno standard della comunità grazie al BIP 39.

Per trasferire un seed, e gli indirizzi da questo creati, da un wallet ad uno di un diverso sviluppatore, potrebbe non essere sufficiente il solo seed (o la sua rappresentazione tramite chiave mnemonica), ma potrebbe essere necessario anche il Derivation Path.

Seed Recovery Phrase

Livello: intermedio

Argomento: tecnologia

La Seed Recovery Phrase, chiamata anche Backup seed phrase o Recovery seed, è una frase mnemonica che rappresenta una chiave privata con funzioni di seed (dall'inglese, "seme") dalla quale il wallet può generare numerose chiavi derivate per le quali non è necessario memorizzare nuove chiavi.

Per la protezione delle seed phrase, il consiglio è quello di scriverle su un foglio di carta e di conservarle in un luogo sicuro. Tuttavia, in genere si sconsiglia agli utenti di conservare le seed phrase memorizzate in file di testo sui propri computer o dispositivi mobili. I computer e smartphone possono essere compromessi da virus, e la memorizzazione su cloud può essere compromessa se

l'account dell'utente viene violato. La pratica migliore per mantenere al sicuro le seed phrase è quindi quella di tenerle offline.

Un modo per effettuare un backup più sicuro della Seed Recovery Phrase è il Shamir backup, che viene offerto come opzione anche da alcuni wallet.

La Seed Recovery Phrase ègeneralmente composta da 12, 18 o 24 parole. Un recovery seed di 12 parole fornisce 128 bit di entropia, che è più che sufficiente per la sicurezza delle chiavi private.
Bitcoin con l'utilizzo della crittografia a curva ellittica, anche se le chiavi private sono a 256 bit, ha la sicurezza della curva ellittica che è circa 128 bit per la curva secp256k1 utilizzata.
Quindi se le 12 parole sono state generate con una buona fonte di entropia, soddisfano gli standard di sicurezza.

segnet

Livello: avanzato

Argomento: tecnologia

Segnet, o The Segregated Witness Testnet, è una testnet Bitcoin che è stata creata per testare nuove funzionalità e modifiche al protocollo Bitcoin.
È stata lanciata nel 2016, principalmente per aiutare nello sviluppo e nel test di Segregated Witness, e utilizza una blockchain separata dalla blockchain principale di Bitcoin.

Segnet viene utilizzata da sviluppatori e ricercatori per testare nuove funzionalità senza interferire con la rete Bitcoin principale. Ad esempio, Segnet è stata utilizzata per testare la SegWit, una modifica al protocollo Bitcoin che ha consentito di ridurre le dimensioni delle transazioni.

Segnet è anche utilizzata per testare nuove versioni del software Bitcoin.

Segnet è un'importante risorsa per la comunità Bitcoin. Permette agli sviluppatori e ai ricercatori di testare nuove funzionalità e modifiche al protocollo Bitcoin in un ambiente sicuro e controllato.

SegWit

Acronimo di: Segregated Witness

Livello: intermedio

Argomento: tecnologia

SegWit, o nella forma estesa Segregated Witness, è un aggiornamento al protocollo bitcoin attivato nel 2017 in modalità soft-fork, e quindi garantendo la retro-compatibilità.

Con l'aggiornamento sono state introdotte diverse novità e sistemati alcuni problemi.

Uno dei cambiamenti più evidenti è stata l'introduzione di un nuovo tipo di indirizzi, che sono riconoscibili per il fatto che iniziano con i caratteri **bc1**, poiché utilizzano come codifica il formato bech32, rispetto ai vecchi indirizzi chiamati legacy che utilizzano la codifica Base58.

SegWit ha risolto il problema della Transaction Malleability. Questo aggiornamento ha aperto la strada all'implementazione di Lightning Network e al più recente aggiornamento Taproot. SegWit ha introdotto due nuovi tipi di script, o modalità di invio e ricezione di bitcoin.

Il nome Segregated Witness deriva dal fatto che le informazioni di una transazione sono state divise in due segmenti e una di queste, ovvero i dati della firma chiamati witness, viene separata dalla parte originale e spostata o segregata come struttura separata alla fine del blocco.

Questo ha permesso di includere più transazioni in ogni blocco, il che ha allentato la pressione sulle fee e ha fornito una parziale soluzione al problema della scalabilità.

La discussione che ha proceduto la decisione di effettuare l'aggiornamento a SegWit è stata controversa e la sua attivazione ha causato profonde divisioni all'interno della comunità Bitcoin. Tuttavia, Bitcoin è emerso più forte e più scalabile, dimostrando che il suo decentramento potrebbe resistere a un tentativo di acquisizione da parte di miner e leader della comunità.

Sebbene SegWit sia tecnicamente un soft fork, ha alterato una delle importanti regole di consenso di Bitcoin in modo retrocompatibile al fine di aumentare il numero di transazioni che potrebbero essere incluse in ciascun blocco.

Prima di SegWit, ogni blocco era limitato a 1 MB di dati, che equivale a circa 1650 transazioni in un blocco pieno. SegWit ha introdotto il Block weight o peso del blocco, che ha sostituito la Block Size o dimensione del blocco come fattore limitante per un blocco. Oggi, i blocchi pieni riescono a contenere circa 2700 transazioni.

Seigniorage

Signoraggio

Livello: avanzato

Argomento: finanza

Il signoraggio rappresenta un concetto fondamentale nell'ambito dell'economia monetaria, storicamente inteso come il profitto derivante dall'emissione di moneta. Tradizionalmente, questo beneficio è stato strettamente legato al potere delle entità sovrane di coniare monete e, in tempi moderni, delle banche centrali di emettere valute fiat. L'emergere di valute digitali decentralizzate come

Bitcoin ha introdotto un nuovo paradigma nel sistema monetario globale, sfidando concetti economici consolidati.

Il concetto tradizionale di signoraggio, applicato alle valute fiat emesse da autorità centrali, può essere applicato ad una criptovaluta decentralizzata con un'offerta limitata e priva di un emittente centrale come Bitcoin, deterrminando se e come la nozione di signoraggio possa essere applicata a Bitcoin, esplorando interpretazioni alternative e confrontando i meccanismi di generazione di valore nei due sistemi. La struttura del rapporto prevede inizialmente la definizione di signoraggio nel contesto finanziario ed economico, seguita dall'analisi delle sue dinamiche nei sistemi di valuta fiat.

Definizione di Signoraggio nella Finanza e nell'Economia Tradizionale

Il termine "signoraggio" affonda le sue radici nel vocabolo francese "seigneur," che significa signore. Storicamente, si riferiva al diritto dei signori feudali o dei sovrani di coniare monete e di trarre profitto da tale attività. Questo profitto poteva derivare dalla deduzione di una tassa sulla quantità di metallo prezioso portata alla zecca per la coniazione o, in alcune epoche, dalla pratica di svalutare la moneta sostituendo parte del metallo prezioso con metalli meno nobili, mantenendo però lo stesso valore nominale.

Nella sua accezione economica moderna, il signoraggio è comunemente definito come il reddito o profitto che i governi o le banche centrali ottengono dall'emissione di moneta. Questo profitto scaturisce tipicamente dalla differenza tra il valore nominale della moneta e il costo sostenuto per la sua produzione e distribuzione. La Banca d'Italia, ad esempio, definisce il signoraggio come "l'insieme dei redditi derivanti dall'emissione di moneta". Altrove viene descritto come "la differenza tra il valore nominale del denaro… e il costo per produrlo". In una prospettiva più ampia, il signoraggio può essere inteso come le risorse reali che uno Stato guadagna quando stampa moneta per acquistare beni e servizi.

È importante menzionare concetti correlati come la "tassa da inflazione," dove il signoraggio, ottenuto attraverso l'aumento dell'offerta di moneta, può portare all'inflazione, agendo di fatto come una tassa sui detentori della valuta esistente. Si distingue inoltre tra signoraggio primario, derivante dall'emissione di base monetaria, e signoraggio secondario, legato ai profitti delle banche commerciali attraverso la creazione di credito ; tuttavia, questo rapporto si concentrerà principalmente sulla definizione primaria pertinente all'emissione di valuta. L'evoluzione storica e le definizioni moderne evidenziano come il signoraggio sia intrinsecamente legato al potere di creare e immettere moneta nell'economia, con un beneficio che tradizionalmente spetta all'autorità emittente. Questa centralizzazione del potere e del profitto è un aspetto cruciale che differenzia i sistemi di valuta fiat da modelli decentralizzati come Bitcoin.

Le Meccaniche del Signoraggio nei Sistemi di Valuta Fiat Tradizionali Nei moderni sistemi di valuta fiat, l'autorità di emettere banconote è generalmente conferita alle banche centrali (come la Federal Reserve negli Stati Uniti o la Banca Centrale Europea), mentre i governi spesso mantengono il controllo sull'emissione di monete metalliche. Le banche centrali creano moneta, in molti casi, attraverso l'acquisto di titoli di stato, un'operazione che immette liquidità nel sistema economico.

Il profitto derivante dal signoraggio si manifesta chiaramente nel fatto che il valore nominale della valuta fiat supera di gran lunga il costo della sua produzione. Ad esempio, la produzione di una banconota da un dollaro statunitense costa pochi centesimi, generando un signoraggio di quasi un dollaro. È interessante notare che, in alcune circostanze, come nel caso del penny statunitense, il costo di produzione può superare il valore nominale, determinando un signoraggio negativo.

Il reddito generato dal signoraggio di solito affluisce alla banca centrale, e una porzione di questi profitti viene spesso trasferita al governo, contribuendo alle finanze pubbliche. Questa entrata può essere utilizzata per finanziare la spesa pubblica, potenzialmente riducendo la necessità di ricorrere alla tassazione.

Il signoraggio può anche essere influenzato e utilizzato come strumento di politica monetaria. L'aumento dell'offerta di moneta attraverso operazioni come il quantitative easing (QE), in cui le banche centrali acquistano obbligazioni governative o altri strumenti finanziari, può essere visto come un modo per sfruttare il signoraggio.

Tuttavia, un'eccessiva creazione di moneta al fine di ottenere maggiori entrate da signoraggio può portare a un aumento dell'offerta di moneta che supera la crescita economica, innescando inflazione e una conseguente diminuzione del potere d'acquisto della valuta detenuta dal pubblico. Questo evidenzia il delicato equilibrio che le banche centrali devono mantenere tra la generazione di entrate per il governo e la stabilità del valore della moneta. La fiducia del pubblico nel governo emittente è fondamentale per il valore della valuta fiat , e la capacità delle banche centrali di controllare l'offerta di moneta è cruciale per mantenere questa fiducia e gestire l'inflazione. La relazione tra le entrate governative derivanti dal signoraggio e il potenziale rischio di inflazione rappresenta una sfida fondamentale nella gestione delle valute fiat.

Bitcoin: Creazione e Distribuzione Bitcoin viene creato attraverso il processo noto come mining, che consiste nella verifica delle transazioni e nella loro aggiunta alla blockchain, il registro digitale distribuito di tutte le transazioni Bitcoin.

Come ricompensa per il loro lavoro, i miner ricevono un certo numero di nuovi bitcoin (il block reward) e le commissioni di transazione incluse nel blocco che hanno validato.

L'Applicabilità del Concetto Tradizionale di Signoraggio a Bitcoin Il concetto tradizionale di signoraggio si basa sull'esistenza di un'autorità centrale (governo o banca centrale) che emette valuta e trae profitto dalla differenza tra il valore nominale e il costo di produzione. Una caratteristica fondamentale di Bitcoin è l'assenza di tale autorità centrale responsabile della sua emissione.

Il "profitto" derivante dalla creazione di nuovi bitcoin (il block reward) non va a un'entità centrale, ma a miner decentralizzati. Questi miner, a loro volta, sostengono costi significativi per l'hardware e l'energia elettrica necessari per partecipare al processo di mining e garantire la sicurezza della rete. La ricompensa che ricevono può essere vista più come un compenso per il loro lavoro e per i costi sostenuti, piuttosto che come un puro profitto da emissione nel senso tradizionale del signoraggio.

La creazione di nuovi bitcoin è un processo decentralizzato, guidato dalla competizione tra i miner, e non una decisione centralizzata presa da un'autorità monetaria. Pertanto, la definizione tradizionale di signoraggio, come profitto guadagnato da un governo o da una banca centrale attraverso l'emissione di valuta a un costo inferiore al suo valore nominale, non si applica direttamente a Bitcoin. Non esiste un'entità sovrana che trae profitto dall'emissione di nuove monete. La natura decentralizzata dell'emissione di Bitcoin e la distribuzione delle ricompense ai miner distinguono fondamentalmente Bitcoin dai sistemi di valuta fiat, dove il signoraggio rappresenta una forma di generazione di entrate centralizzata.

Esplorazioni Alternative del "Signoraggio" in Relazione a Bitcoin Sebbene il concetto tradizionale di signoraggio non si applichi direttamente a Bitcoin, è possibile esplorare interpretazioni alternative che catturino l'idea di valore creato e distribuito all'interno del suo ecosistema.

Una di queste interpretazioni è considerare le ricompense (block reward e commissioni di transazione) ottenute dai miner come una forma di "signoraggio digitale". Questa ricompensa incentiva la manutenzione e la sicurezza della rete decentralizzata, svolgendo una funzione analoga al ruolo di una banca centrale nel mantenimento di un sistema di valuta fiat. È significativo notare che alcune società di mining utilizzano il termine "signoraggio" per descrivere la redditività delle loro operazioni.

Un'altra prospettiva è considerare il valore creato per i primi adottanti di Bitcoin. Coloro che hanno acquisito bitcoin quando il suo valore era trascurabile hanno beneficiato del significativo apprezzamento del suo prezzo nel tempo. Questo guadagno, pur non derivando direttamente dall'emissione di nuove monete, può essere visto come una forma di "signoraggio" per coloro che hanno assunto i primi rischi e contribuito alla crescita della rete.

Si può anche considerare il valore complessivo catturato dalla rete Bitcoin come sistema monetario decentralizzato. La crescente capitalizzazione di mercato e l'adozione rappresentano una forma di "signoraggio" per l'intero ecosistema,

beneficiando i detentori e gli utenti. Questa interpretazione si concentra sul valore creato e acquisito dal protocollo stesso, piuttosto che da una specifica entità.

Nel contesto delle stablecoin emesse su blockchain (come Bitcoin attraverso protocolli come Liquid), si parla di "crypto seigniorage". In questo caso, algoritmi regolano l'offerta per mantenere la stabilità del prezzo, e i profitti derivanti da queste regolazioni possono essere definiti signoraggio. Sebbene non riguardi direttamente l'emissione di Bitcoin, è un concetto correlato nell'ambito delle criptovalute.

Queste interpretazioni alternative suggeriscono che, pur discostandosi dalla definizione tradizionale, l'idea di un beneficio economico derivante dalla creazione e dalla manutenzione di un sistema monetario può essere applicata a Bitcoin, sebbene con meccanismi e beneficiari diversi.

Confronto e Contrasto tra Signoraggio nel Sistema Fiat e Bitcoin

Caratteristica	Sistema di Valuta Fiat	Sistema Bitcoin
Autorità Emittente	Banca Centrale/Governo	Rete Decentralizzata (miner)
Beneficiario del Signoraggio	Governo/Banca Centrale	Miner, Primi Adottanti, Rete
Scopo del Signoraggio	Entrate governative, politica monetaria	Incentivare la sicurezza e la validazione delle transazioni, premiare i primi utilizzatori
Meccanismo	Valore nominale - costo di produzione	Ricompense per blocco + commissioni di transazione, apprezzamento del valore
Controllo	Centralizzato	Decentralizzato
Offerta	Elastica, gestita	Fissa (21 milioni), controllata algoritmicamente

Il confronto tra i due sistemi evidenzia una differenza fondamentale nel controllo e nella distribuzione del signoraggio. Nei sistemi fiat, il signoraggio è un meccanismo centralizzato di profitto per le autorità emittenti, utilizzato per finanziare la spesa pubblica e attuare la politica monetaria. In Bitcoin, invece, il valore derivante dalla creazione di nuova moneta è distribuito in modo decentralizzato ai miner che contribuiscono alla sicurezza della rete e, in parte, ai primi utilizzatori che hanno creduto nel progetto.

Lo scopo del signoraggio è diverso nei due sistemi. Nelle valute fiat, serve principalmente come fonte di entrate per il governo e come strumento per influenzare l'economia. In Bitcoin, il "signoraggio" (nelle sue interpretazioni alternative)

funge da incentivo per la sicurezza della rete e come ricompensa per l'adozione precoce.

Il meccanismo di generazione del valore è anch'esso differente. Nelle valute fiat, il signoraggio deriva principalmente dalla differenza tra il costo di produzione e il valore nominale. In Bitcoin, si manifesta attraverso le ricompense per il mining e l'apprezzamento del valore dovuto alla scarsità e agli effetti di rete.

Infine, la natura centralizzata del controllo nei sistemi fiat contrasta con la decentralizzazione di Bitcoin. L'offerta di valuta fiat è elastica e gestita dalle banche centrali, mentre l'offerta di Bitcoin è fissa e controllata da un algoritmo predefinito. Queste differenze riflettono le diverse filosofie e architetture alla base dei due sistemi monetari.

1. Conclusione: Rivalutare il Signoraggio nell'Era delle Valute Decentralizzate

In sintesi, questo rapporto ha analizzato il concetto di signoraggio in relazione a Bitcoin. Sebbene la definizione tradizionale di signoraggio, come profitto derivante dall'emissione di moneta da parte di un'autorità centrale, non si applichi direttamente a Bitcoin a causa della sua natura decentralizzata e dell'assenza di un emittente centrale che cerca profitto, il concetto di beneficio economico derivante dalla creazione e dalla manutenzione di un sistema monetario rimane rilevante.

Abbiamo esplorato interpretazioni alternative di "signoraggio" all'interno dell'ecosistema Bitcoin, come le ricompense per i miner e l'apprezzamento del valore per i primi adottanti. Queste interpretazioni evidenziano come il valore venga creato e distribuito in modo diverso nei sistemi decentralizzati rispetto ai modelli tradizionali.

Le implicazioni delle valute digitali decentralizzate come Bitcoin per i concetti economici tradizionali sono significative. Il modello Bitcoin offre una prospettiva unica su come un sistema monetario possa essere protetto e come il beneficio derivante dalla sua creazione possa essere distribuito senza fare affidamento sulle tradizionali autorità centralizzate.
Sebbene il termine "signoraggio" possa necessitare di una rivalutazione o di un adattamento quando applicato a Bitcoin, il principio sottostante del beneficio economico derivante dalla creazione e dalla manutenzione di un sistema monetario rimane un elemento chiave per comprendere le dinamiche di queste nuove forme di denaro. Il modello Bitcoin dimostra come questo beneficio possa essere distribuito e come una rete monetaria possa essere protetta senza affidarsi alle tradizionali autorità centralizzate.

Selfish Mining

Livello: avanzato

Argomento: tecnologia

Il Selfish Mining, letteralmente il mining egoista, considerato anche un attacco e quindi chiamato Selfish Mining Attack, è una strategia di mining tramite la quale un miner o un gruppo di miner coordinati risolve un hash e crea un nuovo blocco valido ma invece di pubblicarlo alla rete e aggiungerlo alla blockchain, lo nasconde dalla blockchain pubblica. Questa azione crea un fork.

Non trasmettendo subito il proprio blocco, questi miner creano di fatto il proprio ramo privato della blockchain. Il resto della rete continua a basarsi sul blocco precedente, mentre il selfish miner costruisce in cima a questa nuova catena. Da quel momento, le due catene avranno un aspetto completamente diverso. L'obiettivo del selfish miner è quello di rimanere sempre almeno un blocco avanti rispetto al resto della rete. I nodi accettano la catena con il maggior numero di prove di lavoro accumulate come blockchain valida. In qualsiasi momento, il selfish miner può rivelare la propria catena. Se è considerata più lunga di quella seguita dal resto della rete, i blocchi esistenti saranno scartati e le transazioni invertite. Il miner raccoglie tutte le ricompense da questi blocchi e fa sì che gli altri sprechino risorse. Il successo del selfish mining dipende in parte dalla fortuna, ma soprattutto dalla potenza di hashing a disposizione del miner (nota anche come hash rate). Gli autori del documento osservano che, poiché i miner della catena pubblica non vogliono sprecare risorse, si uniranno ai miner selfish della catena alternativa. A lungo termine, il selfish mining potrebbe minare la decentralizzazione di Bitcoin, in quanto concentra la potenza di hashing in pool più piccoli.

Questa strategia dannosa è stata ampiamente studiata per il Bitcoin. Il selfish mining è un attacco contro l'algoritmo di Difficulty Adjustment, regolazione della difficoltà.

Proposto per la prima volta dai ricercatori della Cornell nel 2013, il "selfish mining" definisce un meccanismo che consente ai miner di collaborare e aumentare i propri profitti creando fork separati e non rivelando i blocchi estratti al resto della rete. Questo ha un impatto sulla salute complessiva del protocollo, poiché la collusione aumenta il rischio di centralizzazione.

Il mining di Bitcoin dipende da una serie di fattori, tra cui, ma non solo, l'efficienza delle macchine di mining, il costo dell'elettricità e la potenza di hash apportata alla rete. Il progetto assicura la decentralizzazione concedendo ricompense ai singoli miner sulla blockchain, il che è una delle ragioni della popolarità dei pool di mining, in quanto consente ai miner di ricevere ricompense continue e costanti. I miner possono ottimizzare notevolmente l'estrazione e aumentare il rendimento impegnandosi in un'attività di Selfish Mining. Se smettono di dichiarare nuovi blocchi alla rete pubblica, possono velocizzare il processo e ridurre lo spreco di risorse.

I fork saranno più piccole della blockchain pubblica, ma i miner possono assicurarsi che i miner della blockchain pubblica lascino la propria chain e si uniscano a quella fork, programmando la rivelazione di nuovi blocchi. Questo processo continua fino a quando la chain fork è più grande della chain originale ed è più

redditizia da minare. Questo può portare la chain fork a diventare più dominante di quella originale, compromettendo gravemente la decentralizzazione.

Il selfish mining non è una strategia praticabile a lungo termine perché, in caso di successo, i miner avrebbero ridotto il valore dei loro token danneggiando la fiducia del pubblico nella criptovaluta. Inoltre, se tutti i miner si impegnano nella stessa attività, è probabile che nessuno ne tragga un vantaggio considerevole.

Nel 2018, Jake Gober ha teorizzato che se il selfish mining fosse più redditizio dell'honest mining, molti minatori lo farebbero. Jake ha dimostrato che, sebbene il selfish mining sia più redditizio dell'honest mining, più minatori o gruppi egoisti su una rete creerebbero una gara tra i fork e ridurrebbero la redditività.

Zhaojie Wang et al. osservano nella loro ricerca che alla fine del 2021 non erano noti casi di attacchi di selfish mining nel mondo reale.

Le argomentazioni di entrambe le parti suggeriscono che gli attacchi di selfish mining possono verificarsi, ma potrebbero essere puramente accademici. Un'altra possibilità è che un attacco di selfish mining si sia già verificato in passato, ma non sia stato osservato.

È più probabile, invece, che la maggior parte dei miner abbia intenzioni oneste e che la modellazione matematica venga utilizzata per spingere lo sviluppo della tecnologia blockchain.

Sell Wall

Livello: intermedio

Argomento: finanza

Letteralmente Muro di Vendita. Si verifica quando uno o più trader mette in vendita una moneta a un determinato prezzo e non ci sono sufficienti ordini di acquisto in quel exchange per superare quel prezzo.

SEPA

Acronimo di: Single Euro Payments Area

Area unica dei pagamenti in euro

Livello: intermedio

Argomento: politica

I bonifici SEPA sono il metodo standard per inviare denaro tramite bonifico all'interno della zona Euro.

La SEPA, Single Euro Payments Area ovvero l'Area unica dei pagamenti in euro, è una rete paneuropea che permette l'invio e la ricezione di pagamenti tra due conti correnti situati in due paesi diversi.

Il bonifico SEPA si basa sul codice IBAN del conto corrente per indirizzare le transazioni europee domestiche, prima del 2016 era necessario anche il codice BIC.

Sequential deterministic wallets

Wallet deterministici sequenziali

Livello: intermedio

Argomento: tecnologia

I wallet deterministici sequenziali prendono una singola frase seme/passphrase e la incrementano ripetutamente per generare nuove coppie di chiavi. Ciò significa che è sufficiente solo memorizzare gli indirizzi e quindi rigenerare le chiavi private quando necessario.

SHA-256

Livello: intermedio

Argomento: tecnologia

Una funzione di hash crittografica che genera una firma a 256 bit per un testo, utilizzata in Bitcoin Proof-of-Work (PoW). Stando a "Secure Hash Algorithm", è uno degli algoritmi SHA-2, inizialmente progettato dalla NSA.

Shamir backup

Livello: avanzato

Argomento: tecnologia

Il Shamir backup è una modalità per effettuare copie di sicurezza per contrastare i due maggiori rischi legati alla protezione del recovery seed: il furto e la distruzione.

Il Shamir backup è un metodo di protezione delle password o di altre informazioni sensibili mediante la creazione di un insieme di *parti* o *pezzi* (share) che possono essere utilizzati per ricostruire l'informazione originale. Questo metodo, chiamato SSS o Shamir's Secret Sharing, è stato sviluppato dal matematico israeliano Adi Shamir, che ha dato il suo nome all'algoritmo.

Il funzionamento del Shamir backup è il seguente: prima di tutto, l'informazione da proteggere viene suddivisa in un certo numero di parti, chiamate *shares*. Ogni parte è quindi distribuita a un soggetto diverso o conservata in un posto diverso. Per ricostruire l'informazione originale, è necessario ottenere un certo numero

di queste parti denominato soglia o *threshold*, che possono essere combinate per ottenere l'informazione completa. La sicurezza di questo metodo dipende dal numero di parti necessarie per ricostruire l'informazione originale e dal fatto che le parti distribuite a diverse persone o enti non possono essere utilizzate per ricostruire l'informazione da sole.

Il Shamir backup viene spesso utilizzato per proteggere le password o le chiavi private di accesso ai portafogli di criptovalute, poiché offre un modo sicuro per proteggere queste informazioni sensibili senza doverle memorizzare o archiviare in modo centralizzato. Tuttavia, il Shamir backup può essere utilizzato anche per proteggere altre informazioni sensibili, come le chiavi di accesso ai sistemi di sicurezza o i codici di autenticazione per l'accesso ai servizi online.

Il recovery seed è la chiave del vostro patrimonio digitale e se lo si perde, le proprie criptovalute potrebbero andare irrimediabilmente perse. Per evitarlo, è possibile creare più parti, o share, per effettuare il backup delle chiavi private e specificare un numero prestabilito (denominato soglia o threshold) di queste share uniche che devono essere raccolte e utilizzate per recuperare il wallet. Questo è il principio di base del backup di Shamir.

Semplificando, ipotizziamo ad esempio che il nostro seed backup sia formato dalle parole:

`abisso babele catena datato elfico fanale`

Queste parole potrebbero essere suddivise in 3 shares, con una soglia o threshold di 2 shares:

- share 1: `abisso babele catena datato XXXXXX XXXXXX`
- share 2: `abisso babele XXXXXX XXXXXX elfico fanale`
- share 3: `XXXXXX XXXXXX catena datato elfico fanale`

ognuna di queste share andrebbe conservata in un posto diverso, nessuno trovando una sola share potrebbe ricostruire l'elenco completo delle parole, ma se anche una delle share dovesse andar persa si potrebbe ricostruire il messaggio con le altre due.

Questo esempio è una semplificazione del metodo Shamir's Secret Sharing, attraverso il quale si possono un numero arbitrario di share e un valore arbitrario del threshold (ma inferiore alle share), e si può applicare ad un qualunque messaggio sul quale effettuare un algoritmo di crittografia.

Sharding

Livello: avanzato

Argomento: tecnologia

È un concetto ampiamente utilizzato nei database per renderli più efficienti e implica la creazione di frammenti (shards) da una parte più grande. Il partizionamento viene eseguito orizzontalmente anziché verticalmente e ogni frammento

viene memorizzato nei vari nodi. Questo estende il carico e rende il database più efficiente. Nel caso della blockchain, ogni nodo avrà quindi solo una parte dei dati sulla blockchain, e non l'intera informazione. I nodi che mantengono un frammento espongono le informazioni in modo condiviso solo relativamente a quel frammento, quindi la decentralizzazione è mantenuta: tuttavia, ogni nodo non è obbligato a caricare le informazioni sull'intera blockchain, contribuendo così alla scalabilità.

Shilling

shillare

Livello: intermedio

Argomento: finanza

Shilling, che in italiano viene reso con il neologismo "shillare" è un gergo che ha radici nel campo del marketing e dell'advertising, ed è utilizzato per descrivere l'atto di promuovere o pubblicizzare in modo eccessivamente entusiastico un prodotto, un servizio o un'idea.

Inizialmente aveva una accezzione negativa, indicando spesso senza rivelare in modo trasparente il proprio interesse personale o finanziario nella promozione stessa. In sostanza, uno "shill" è una persona che fa pubblicità o propaganda in modo falso o esagerato.

Nel contesto delle criptovalute e del settore delle cripto, il termine "shillare" è spesso utilizzato per riferirsi alle persone o agli influencer che promuovono specifiche criptovalute o progetti legati alle criptovalute in modo eccessivamente positivo, senza fornire informazioni obiettive o senza rivelare conflitti di interesse. Questo può accadere su social media, forum, blog, video online e in altri canali di comunicazione.

L'obiettivo degli "shill" nel contesto delle criptovalute potrebbe essere quello di aumentare il prezzo di una criptovaluta in modo da trarne profitto dalle proprie posizioni, indipendentemente dalla reale qualità o valore del progetto. Questa pratica è spesso vista in modo negativo, poiché può ingannare gli investitori meno esperti e portare a decisioni finanziarie errate.

Shitcoin

Livello: base

Argomento: finanza

Un dispregiativo per indicare una moneta senza un potenziale valore o prodotto funzionante. I massimalisti bitcoin considerano shitcoin tutte le altcoin, ovvero tutte le cripto diverse da bitcoin.

Short

Vendita allo scoperto

Livello: base

Argomento: finanza

Short, Shorting o Short selling, in italiano vendita allo scoperto, chiamata anche vendita a nudo, è un'operazione che consiste nella vendita di asset, titoli o coin non direttamente posseduti dal venditore, ma presi in prestito dietro il versamento di un corrispettivo, con l'intenzione di riacquistarlo o coprirlo in seguito a un prezzo inferiore. Consiste nello scommettere su un movimento ribassista dei prezzi di strumenti finanziari non posseduti e quindi nella loro vendita quando il prezzo è ritenuto alto e successivamente nel loro riacquisto quando il prezzo sarà più basso.

Quando un trader ritiene che il prezzo un certo titolo diminuirà nel prossimo futuro, può decidere di venderlo allo scoperto. Lo short selling è una strategia di investimento che consente al trader di ottenere un'esposizione negativa a un'attività. Con questa tecnica un trader prende in prestito un asset per venderlo, con l'aspettativa che il prezzo continui a scendere. Nel caso in cui il prezzo diminuisca, il venditore allo scoperto acquisterà l'asset a questo prezzo più basso per restituirlo al prestatore dell'asset, realizzando la differenza di profitto. Tuttavia, se il prezzo di un titolo shortato sale, il venditore allo scoperto è responsabile della differenza e può subire perdite finanziarie, e può anche essere costretto a chiudere le proprie posizioni.

Il venditore allo scoperto dovrà poi acquistare l'asset per restituirlo al proprietario originario. Se l'asset è più economico al momento dell'acquisto rispetto a quello della vendita, il venditore allo scoperto ha realizzato un profitto. I venditori allo scoperto perdono denaro se l'asset che hanno shortato sale di valore prima che lo acquistino. Poiché il prezzo di un'attività può aumentare senza un limite massimo, un venditore allo scoperto ha un numero illimitato di perdite potenziali. Al contrario, la maggior parte delle attività detenute in una posizione long non può valere meno di 0 dollari.

Quando gli investitori con posizioni short sono costretti a chiudere le proprie posizioni, si può verificare il fenomeno chiamato Short Squeeze, una condizione insolita che provoca un rapido aumento dei prezzi del titolo.

Short Squeeze

Livello: avanzato

Argomento: finanza

Uno short squeeze è un fenomeno nel trading che si verifica quando gli investitori con posizioni short sono costretti a chiudere le proprie posizioni. Se il valore dell'attività allo scoperto aumenta in modo significativo, le posizioni short

perderanno gran parte del loro valore. Le posizioni short alla fine saranno chiuse per evitare ulteriori perdite. Per chiudere le posizioni, gli short dovranno riacquistare l'asset, aumentando la domanda e il prezzo dell'asset. L'aumento del prezzo può avere un effetto domino, costringendo ulteriori short a chiudere le loro posizioni che a loro volta aumentano ulteriormente il prezzo. Il rapido aumento dei prezzi dovuto a uno short squeeze che deriva da prezzi già elevati si traduce in condizioni di trading estreme per un asset. Gli asset che subiscono una short squeeze possono far deviare i loro prezzi in modo significativo dal valore sottostante dell'asset. Le short squeeze si traducono anche in una volatilità significativa.

Una short squeeze è una condizione insolita che provoca un rapido aumento dei prezzi di un'azione o di un altro titolo negoziabile. Affinché si verifichi uno short squeeze, il titolo deve avere un grado insolito di venditori allo scoperto che detengono posizioni al suo interno. La short squeeze inizia quando il prezzo sale inaspettatamente. La condizione si manifesta come una misura significativa del fatto che i venditori allo scoperto decidono casualmente di tagliare le perdite e uscire dalle loro posizioni.

Uno short squeeze accelera l'aumento del prezzo di un titolo quando i venditori allo scoperto si tirano indietro per ridurre le loro perdite. Gli investitori contrarian cercano di anticipare uno short squeeze e acquistano titoli che dimostrano un forte interesse allo short. Sia i venditori allo scoperto che i contrarian fanno mosse rischiose. Un investitore saggio ha ulteriori ragioni per andare allo scoperto o acquistare quel titolo. Lo short sqeeze di GameStop nel gennaio 2021 ha fatto perdere 5 miliardi di dollari ai short seller.

Side Chain

Livello: intermedio

Argomento: tecnologia

Le sidechain, chiamate anche two-way pegged sidechains, sono blockchain la cui unità di valuta nativa è la stessa di un'altra blockchain. Nel contesto di Bitcoin, le sidechain utilizzano un meccanismo in cui i bitcoin vengono depositati in un contratto sulla blockchain di Bitcoin e un numero uguale di bitcoin viene creato sulla sidechain dove potranno essere spesi. Gli utenti della sidechain possono in seguito inviare bitcoin sidechain a un contratto speciale che li distrugge e rilascia una quantità corrispondente dei bitcoin precedentemente depositati al contratto sulla blockchain. Lo scopo è quello di introdurre diversi parametri quali i meccanismi e velocità di mining, o altre esigenze legate ad esempio alla scalabilità.

Alcuni esempi di side-chain basate su Bitcoin sono Liquid, Stacks, Rootstock.

Sighash flag

Livello: avanzato

Argomento: tecnologia

Chi usa Bitcoin di solito dà per scontato che quando si vuole spendere i propri bitcoin, sia sufficiente firmare una transazione con la propria chiave privata.

Questo è vero, ma è una eccessiva semplificazione. Le transazioni Bitcoin possono essere firmate in diversi modi, e questi modi vengono definiti **SIGHASH**. Il Sighash viene codificato nella parte della firma della transazione.

Una signature, firma un hash di dati, e quindi una firma attribuisce certezza ad un pezzo di dati, ovvero ne effettua il commitment. Se i dati vengono modificati dopo la creazione della firma, la firma viene invalidata. Pertanto, una firma è un commitment verso un determinato insieme di dati. Una firma può quindi effettuare il commitment solo ad un sottoinsieme dei dati in una transazione, e questo rende le firme utili per una serie di scenari.

La presenza di più tipi di firma ci permette di creare transazioni innovative che non si limitano a spendere Bitcoin.

Il Sighash flag, flag dell'hash (sighash) della signature o della firma, è una piccola parte di ogni input di una transazione che determina quali parti della transazione diventano immutabili una volta che una firma è stata aggiunta alla transazione.

Bisogna inoltre ricordare che una transazione può avere diversi input, e ogni input può contenere una diversa firma nel suo script di sblocco ScriptSig. Di conseguenza, una transazione che contiene più input può avere firme con flag SIGHASH diversi che effettuano il commit a parti diverse della transazione in ciascuno degli input. Si noti anche che le transazioni bitcoin possono contenere input di diversi "proprietari", che possono firmare solo un input in una transazione parzialmente costruita (e non valida), collaborando con altri per raccogliere tutte le firme necessarie a creare una transazione valida. Molti dei tipi di flag SIGHASH hanno senso solo se si pensa a più partecipanti che collaborano al di fuori della rete bitcoin e aggiornano una transazione parzialmente firmata.

Notare che i flag SIGHASH raramente vengono presentati come opzione nei wallet portafoglio. I wallet che costruiscono gli script P2PKH generalmente li firmano con i flag SIGHASH_ALL. Per utilizzare un flag SIGHASH diverso, può essere necessario scrivere un software per costruire e firmare le transazioni.

Il flag sighash determina su quale insieme di dati all'interno della transazione è stato fatto il commitment, ed esistono tre flag SIGHASH: ALL, NONE e SINGLE.

SIGHASH flag	Valore	Descrizione
ALL	**0x01**	La firma si applica a tutti gli input e gli output
NONE	**0x02**	La firma si applica a tutti gli input, ma a nessun output.
SINGLE	**0x03**	La firma si applica a tutti gli input, ma solo all'output con lo stesso numero di indice dell'ingresso firmato

Inoltre, esiste un flag di modifica SIGHASH_ANYONECANPAY, che può essere combinato con ciascuno dei flag precedenti. Quando ANYONECANPAY è impostato, solo un input viene firmato, lasciando gli altri (e i loro numeri di sequenza) aperti alla modifica. ANYONECANPAY ha il valore 0x80 e viene applicato mediante OR bitwise, ottenendo i flag combinati come mostrato in Tipi di SIGHASH con modificatori e relativi significati.

I valori possibili di Sighash flag sono:

- SIGHASH_ALL = 1
- SIGHASH_NONE = 2
- SIGHASH_SINGLE = 3
- SIGHASH_ANYONECANPAY = 0x80

SIGHASH_ALL Quasi tutte le transazioni utilizzano il flag sighash SIGHASH_ALL, il che significa che la firma di ogni ingresso è valida solo se tutti gli altri input e output rimangono invariati.

Altri flag sighash consentono di mantenere valida la firma di un ingresso anche se altri ingressi o uscite vengono modificati.

SIGHASH_SINGLE All'interno di una transazione, ogni ingresso richiede la propria firma e quindi il proprio flag sighash. Ciò significa che gli input possono essere costruiti in modo flessibile. Quando più parti contribuiscono con gli input a una determinata transazione, possono preoccuparsi solo dei propri output specifici. Ad esempio, se Alice contribuisce con 1 BTC a una transazione e si aspetta 1,2 BTC in cambio, probabilmente le interessa solo che il suo output di 1,2 BTC sia garantito alla firma. In questo caso, Alice potrebbe utilizzare il flag SIGHASH_SINGLE. Questo flag impegna tutti gli input, ma solo un singolo output. Ciò consentirebbe alle altre parti della transazione di aggiungere e modificare i propri output a piacimento, purché non alterino l'output di 1,2 BTC di Alice.

SIGHASH_NONE In alternativa, nel raro caso in cui una parte della transazione non si preoccupi di quali siano gli output, può utilizzare il flag Sighash SIGHASH_NONE, che impegna tutti gli input ma non gli output.

SIGHASH_ANYONECANPAY Infine, il flag SIGHASH_ANYONECANPAY assicura che solo l'input in questione sia firmato, mentre gli altri tre flag sighash da soli assicurano che tutti gli input siano firmati. Questo flag sighash può essere combinato con qualsiasi altro flag sighash per controllare quali uscite e quali ingressi sono firmati.

Uso pratico di combinazioni dei Sighash flag

Ecco come alcune combinazioni dei valori di Sighash flag possono essere utilizzate nella pratica:

ALL | ANYONECANPAY Può essere utile per realizzare una transazione in stile "crowdfunding". Chi cerca di raccogliere fondi può costruire una transazione con un singolo output. Il singolo output paga l'importo "obiettivo" al raccoglitore di fondi. Una transazione di questo tipo non è ovviamente valida, poiché non ha input. Tuttavia, altri possono modificarla aggiungendo un proprio input, come donazione. Essi firmano il loro input con ALL|ANYONECANPAY. Se non viene raccolto un numero sufficiente di input per raggiungere il valore dell'output, la transazione non è valida. Ogni donazione è una "promessa", che non può essere riscossa da chi raccoglie i fondi finché non viene raggiunto l'intero obiettivo.

NONE Può essere usato per creare un "assegno al portatore" o un "assegno con destinatario in bianco" di un importo specifico. Questa transazione non verrebbe trasmessa alla rete da chi la crea, ma consegnata a qualcuno senza impostare l'indirizzo di destinazione, e chi la riceve può scrivere il proprio indirizzo bitcoin e riscattare l'importo. Tramite una transazione di questo tipo si può fare il commit sull'input, lasciando la possibilità di modificare il locking script dell'output.

NONE | ANYONECANPAY Può essere usato per costruire un "dust collector", raccoglitore di dust o polvere. Gli utenti che hanno piccoli UTXO nei loro wallet non possono spenderli perché il costo delle fee ne supera il valore. Con questo tipo di firma, le UTXO dust possono essere donati perché chiunque possa aggregarli e spenderli quando vuole.

Evoluzioni future di sighash

In futuro, al protocollo Bitcoin potrebbero essere aggiunti altri flag sighash, per consentire casi d'uso più flessibili, ma per ora solo i quattro sopra citati sono considerati validi.

Esistono già alcune proposte per modificare o espandere il sistema SIGHASH. Una di queste proposte è Bitmask Sighash Modes di Glenn Willen di Blockstream, nell'ambito del progetto Elements. L'obiettivo è quello di creare un sostituto flessibile per i tipi di SIGHASH che consenta "bitmask arbitrarie, riscrivi-

bili dal miner, di ingressi e uscite" in grado di esprimere "schemi contrattuali di preimpegno più complessi, come le offerte firmate con modifica in uno scambio di beni distribuito".

SIGHASH_ANYPREVOUT è la proposta di un nuovo tipo di flag sighash, che firma la maggior parte della transazione, ma non gli input. Ciò significa che gli input possono essere scambiati, purché i nuovi input siano ancora compatibili con la firma.

Signature

Firma

Livello: base

Argomento: tecnologia

Quella parte di una transazione bitcoin che dimostra che la transazione è approvata dal proprietario della chiave privata collegata al bitcoin oggetto della transazione. Analogamente alle impronte digitali, le firme digitali sono uniche per una singola persona o entità. Queste firme sono derivate matematicamente da una speciale coppia di numeri chiamata coppia di chiavi pubblica/privata. Una firma su una chiave pubblica può essere creata solo dal titolare della chiave privata corrispondente. Come una vera firma, una firma digitale ha lo scopo di dimostrare al destinatario che il messaggio è autentico.

sigop

Acronimo di: signature operation

Livello: avanzato

Argomento: tecnologia

Un sigop, abbreviazione di signature operation (operazioni di firma), rappresenta il numero di operazioni di verifica delle firme digitali in una transazione Bitcoin.

È un'unità di misura che quantifica la complessità di una transazione in funzione delle firme digitali elaborate.
Le transazioni bitcoin hanno uno script che consente di effettuare diverse operazioni, questo script ha pochissime funzionalità. Di conseguenza, è abbastanza semplice da eseguire. Tra le varie operazioni che può fare, la verifica della firma è di gran lunga l'operazione più costosa da eseguire. Queste verifiche hanno dei valori di sigop che vengono conteggiati.

Esiste un limite massimo di sigop che possono essere inclusi in un blocco Bitcoin, chiamato MAX_BLOCK_SIGOPS_COST, e un limite massimo per transazione chiamato MAX_STANDARD_TX_SIGOPS_COST.
Prima di segwit, il limite di sigop per blocco era di 20'000, con segwit è stato

portato a 80'000.
Il valore per le transazioni, MAX_STANDARD_TX_SIGOPS_COST, è un quinto di MAX_BLOCK_SIGOPS_COST, quindi una transazione standard può avere al massimo un costo di 16'000 sigop.
Questi limiti evitano che le transazioni diventino troppo complesse da elaborare e per mantenere la scalabilità della rete Bitcoin, ma possono in casi particolari rendere più complesso calcolare le fee ottimali per far confermare velocemente una transazione.

Le operazioni di firma comportano costi diversi a seconda che siano operazioni single o multi-sig e a seconda di dove compaiono in una transazione Bitcoin.

Ecco alcuni esempi di come vengono conteggiati i sigop:

- Una firma digitale standard conta come un sigop di base.
- Una transazione multisig con due firme conta come due sigop di base.
- Una transazione Pay-to-Script-Hash P2SH con una firma conta come un sigop di base.
- Una transazione Pay-to-Witness-Script-Hash P2WSH con una firma conta come un sigop complesso.

La comprensione del limite sigop è importante per gli sviluppatori Bitcoin che creano transazioni e per gli utenti Bitcoin che vogliono comprendere le limitazioni della rete.

Il modo con cui i sigop sono conteggiati dipende dal contesto.

Nello scriptPubKey degli output, e nello scriptSig degli input (quest'ultimo non capita quasi mai, ma quando succede verrà conteggiato):

- OP_CHECKSIG e OP_CHECKSIGVERIFY viene conteggiato come 4
- OP_CHECKMULTISIG e OP_CHECKMULTISIGVERIFY viene conteggiato come 80

Nei redeem script P2SH:

- OP_CHECKSIG e OP_CHECKSIGVERIFY viene conteggiato come 4
- OP_CHECKMULTISIG e OP_CHECKMULTISIGVERIFY viene conteggiato come 4n when preceded by OP_n, e come 80 negli altri casi.

Nei witness script P2WSH:

- OP_CHECKSIG e OP_CHECKSIGVERIFY viene conteggiato come 1
- OP_CHECKMULTISIG e OP_CHECKMULTISIGVERIFY viene conteggiato come n quando preceduto da OP_n, e come 20 negli altri casi.

In P2TR taproot scripts: Non sono conteggiati Sigop.

silent address

Livello: avanzato

Argomento: tecnologia

I silent address sono degli indirizzi che consentono di effettuare dei silent payment Bitcoin.

Un silent address inizia con i caratteri sp1, questo un esempio:

`sp1qqweplq6ylpfrzuq6hfznzmv28djsraupudz0s0dclyt8erh70pgwxqkz2ydatksrdzf770umsntsmcjp4kcz7jqu`

È sufficiente generare un solo indirizzo Silent Payment permanente per poter ricevere pagamenti da diversi utenti. Questo indirizzo unico consente di mantenere la privacy, poiché ogni transazione utilizzerà una chiave pubblica unica, garantendo che ogni pagamento sia indirizzato in modo sicuro e anonimo.

La prima versione dei silent address inizia con `sp1q` ed è chiamata *version 0*.

Effettivo indirizzo di ricezione Quando si effettua un pagamento ad un silent address, nella blockchain bitcoin non viene registrato il silent address ma un indirizzo di ricezione one-time che viene creato dal mittente.

La creazione dell'indirizzo di ricezione viene eseguita interamente dal mittente, e non richiede assolutamente che il destinatario sia online.
L'indirizzo di ricezione è un indirizzo monouso unico di cui solo il destinatario del pagamento controlla le chiavi.

Questo indirizzo effettivo di ricezione è un indirizzo Taproot, unico e monouso che fa apparire il pagamento esattamente come qualsiasi altro pagamento Taproot sulla blockchain, impedendo così a un osservatore esterno di sapere che è stato utilizzato un silent payments, e ancor meno di collegare i pagamenti a un silent address specifico.

Quando Alice vuole inviare fondi al silent address che Bob ha pubblicato, per creare l'indirizzo di ricezione sul quale fare il pagamento utilizza tre chiavi:

1. la chiave pubblica dell'UTXO che Alice vuole inviare a Bob,
2. la chiave pubblica che estrae dal silent address di Bob
3. un segreto condiviso (generato utilizzando la chiave pubblica Silent Payment e la chiave privata UTXO dell'utente usando ECDH) che solo Alice e Bob possono conoscere.

Queste tre chiavi si combinano in un indirizzo Taproot che Bob può quindi validare e spendere, permettendo ad Alice di generare praticamente infiniti indirizzi senza alcuna comunicazione con Bob.

silent payments

Livello: avanzato

Argomento: tecnologia

I Silent Payment (Pagamenti silenziosi) permettono agli utenti di condividere e pubblicare un singolo indirizzo senza sacrificare la privacy, generando una chiave unica che solo il mittente e il destinatario possono identificare.

I Silent Payment permettono di creare un singolo indirizzo statico o silent address, da condividere con amici, usare per donazioni senza sacrificare la privacy. Quando qualcuno vuole inviarti un pagamento, usa la chiave pubblica che fa parte del tuo silent address, la combina con le chiavi pubbliche degli UTXO che vuole inviare e genera un indirizzo unico, monouso che sulla blockchain appare come qualsiasi altro indirizzo Taproot.

I silent payment un tipo di pagamento che può essere effettuato verso un indirizzo on-chain unico per ogni pagamento, anche se il destinatario ha fornito al pagatore un indirizzo riutilizzabile (offchain). Questo aiuta a migliorare la privacy.

Tradizionalmente, un utente che riceve pagamenti dovrebbe generare un nuovo indirizzo Bitcoin per ogni pagamento. Questo perché il riutilizzo degli indirizzi, ovvero ricevere più pagamenti allo stesso indirizzo, è una pessima pratica per la privacy perché rivela che lo stesso utente ha ricevuto quei pagamenti, anche se gli UTXO sono successivamente spesi in transazioni separate.
L'uso di un nuovo indirizzo spesso richiede un'interazione sicura tra mittente e destinatario affinché il destinatario possa fornire un indirizzo nuovo ogni volta. Tuttavia, l'interazione è spesso impraticabile e in molti casi indesiderabile.

Con i silent payment, un destinatario può generare e pubblicare un singolo indirizzo di pagamento silent address, eliminando la necessità di interazione.

I principali vantaggi dei Silent Payment sono:

- Esperienza utente più semplice: gli utenti devono preoccuparsi solo di un singolo indirizzo statico invece di generare nuovi indirizzi per ogni ricezione.
- Migliore privacy per il ricevente: il riutilizzo degli indirizzi con i Silent Payment è impossibile, poiché nessun mittente può generare lo stesso indirizzo sulla blockchain.
- Migliore privacy per il mittente: i riceventi non possono collegare le transazioni dallo stesso mittente, offrendo maggiore privacy anche al mittente.
- Nessun server richiesto: chiunque abbia un wallet che supporta i Silent Payment può ricevere fondi senza riutilizzo degli indirizzi, senza comunicazione e senza gestire infrastrutture complesse.

I silent payment sono definiti nel BIP 352.

Il destinatario del pagamento rileva il pagamento scansionando le transazioni nella blockchain ed eseguendo un calcolo ECDH con le chiavi pubbliche di input sommate della transazione e la chiave di scansione dal loro indirizzo. Il principale svantaggio è che è più dispendioso dal punto di vista computazionale rispetto alla semplice scansione dell'UTXO Set per uno scriptPubKey come nei wallet in

stile BIP32. Inoltre, l'uso di silent payment in un contesto collaborativo come il coinjoining è lasciato per lavori futuri, e rimane una questione aperta se tale collaborazione possa essere resa provatamente sicura.

Silk Road

Livello: intermedio

Argomento: legale

Silk Road era un sito di commercio elettronico nel quale i pagamenti venivano fatti in Bitcoin, accessibile solo tramite la rete anonima Tor, e nel quale era possibile comprare e vendere diversi prodotti considerati a volte illegali quali droghe, documenti falsi, armi.

Simplicity

Livello: avanzato

Argomento: tecnologia

Simplicity è un linguaggio di programmazione per smart contract che è stato proposto come possibile successore del linguaggio di scripting Bitcoin. È stato progettato per essere più efficiente, più sicuro e scalabile del Bitcoin Script. L'obiettivo principale di Simplicity è rendere più agevole la creazione di script complessi e sicuri, riducendo il rischio di errori e vulnerabilità.

Simplicity è un linguaggio di programmazione di tipo funzionale, il che significa che basa il suo funzionamento sul concetto di funzioni. Questo lo rende più semplice da capire e da utilizzare rispetto a un linguaggio di programmazione di tipo imperativo, come il Bitcoin Script.

Simplicity è anche un linguaggio di programmazione sicuro, il che significa che è difficile scrivere codice che possa essere utilizzato per scopi dannosi. Ciò è dovuto al fatto che Simplicity utilizza un sistema di tipi statici, che consente di verificare la correttezza del codice durante la compilazione.

Infine, Simplicity è un linguaggio di programmazione scalabile, il che significa che può essere utilizzato per creare smart contract complessi e di grandi dimensioni. Ciò è dovuto al fatto che Simplicity utilizza un sistema di ottimizzazione che riduce la dimensione del codice durante la compilazione.

Il Bitcoin Script Simplicity è ancora in fase di sviluppo, ma ha il potenziale per migliorare in modo significativo la funzionalità e la sicurezza dei smart contract Bitcoin. Per utilizzare Simplicity su Bitcoin sarà necessario un soft fork e una proposta del genere non è stata ancora avanzata. Attualmente esiste il supporto Simplicity per i rami di test delle basi di codice ElementsProject.org e Bitcoin Core.

Ecco alcuni dei vantaggi di Simplicity rispetto al Bitcoin Script:

- Maggiore efficienza: Simplicity è un linguaggio di programmazione più efficiente del Bitcoin Script, il che significa che richiede meno risorse per essere eseguito.
- Maggiore sicurezza: Simplicity è un linguaggio di programmazione più sicuro del Bitcoin Script, il che significa che è meno vulnerabile a attacchi.
- Maggiore scalabilità: Simplicity è un linguaggio di programmazione più scalabile del Bitcoin Script, il che significa che può essere utilizzato per creare smart contract più complessi e di grandi dimensioni.

Tuttavia, Simplicity ha anche alcuni svantaggi rispetto al Bitcoin Script:

- Maggiore complessità: Simplicity è un linguaggio di programmazione più complesso del Bitcoin Script, il che lo rende più difficile da imparare e da utilizzare.
- Maggiore rigidità: Simplicity è un linguaggio di programmazione più rigido del Bitcoin Script, il che significa che è meno flessibile e meno adattabile a nuove esigenze.

Nel complesso, il Bitcoin Script Simplicity è una tecnologia promettente che ha il potenziale per migliorare in modo significativo la funzionalità e la sicurezza dei smart contract Bitcoin. Tuttavia, è importante essere consapevoli dei vantaggi e degli svantaggi di Simplicity prima di utilizzarlo.

Offre inoltre scripting merklizzato nativo, semantica formale e controllo del tipo.

slashing

Livello: intermedio

Argomento: politica

Lo slashing è un meccanismo punitivo per controllare il comportamento dei validatori nei sistemi PoS.

Il meccanismo di consenso di Ethereum 2.0 prevede un paio di regole volte a prevenire gli attacchi alla rete. Al validatore che infrange le regole viene effettuato lo slashing ed espulso dalla rete. Lo slashing significa che una parte significativa dello stake del validatore viene rimossa: fino all'intero staking nel caso peggiore. Il software del validatore e i staking provider avranno una protezione integrata contro gli slash accidentali. Lo slashing dovrebbe riguardare solo i validatori che si comportano in modo scorretto e deliberato.

A seguito delle sanzioni dell'OFAC del governo degli Stati Uniti nei confronti degli indirizzi legati a Tornado Cash ad agosto 2022, la comunità di Ethereum si è divisa su come rispondere alla minaccia della censura delle transazioni a livello di protocollo dopo che il miner Ethereum, Ethermine, ha deciso di non elaborare le transazioni dello strumento di privacy Tornado Cash, spingendo i membri della comunità a preoccuparsi di cosa accadrebbe se altri validatori centralizzati facessero lo stesso. Come possibilie risposta alla minaccia di censura delle transazioni su Ethereum è stato suggerito il social slashing. Alcuni la

definiscono una “trappola” che farà più male che bene, mentre altri affermano che è necessaria per fornire “proprietà credibili di neutralità e resistenza alla censura” su Ethereum. La strategia potrebbe portare a una divisione della chain con alcuni validatori che elaborano le transazioni sulla chain priva di censura e gli altri che convalidano solo la chain che censura le transazioni secondo quanto richiesto dagli organi di alcuni governi.

Slippage

Livello: avanzato

Argomento: finanza

Lo slippage (slittamento) è un termine utilizzato nel trading per descrivere la differenza tra il prezzo previsto di un ordine e il prezzo effettivo al quale l'ordine viene eseguito. In altre parole, lo slippage rappresenta la differenza tra il prezzo a cui un trader ha piazzato un ordine e il prezzo a cui l'ordine è stato effettivamente eseguito. Ciò può accadere quando c'è una grande volatilità del mercato o quando c'è una scarsità di liquidità per un determinato strumento finanziario.

Per esempio, se un trader vuole acquistare 100 azioni a un prezzo di $10 ma alla fine l'ordine viene eseguito a $10,05, allora lo slippage è di $0,05 per azione. In generale, lo slippage negativo indica che l'ordine è stato eseguito a un prezzo migliore di quello previsto, mentre lo slippage positivo indica che l'ordine è stato eseguito a un prezzo peggiore di quello previsto.

Lo slippage può verificarsi per diversi motivi. Nella maggior parte dei casi, è dovuto alle condizioni di mercato volatili. I mercati possono essere volatili in base a eventi di mercato, come una pubblicazione degli utili, un annuncio di politica monetaria o la volatilità. In altri casi, lo slippage può verificarsi per una serie di altri motivi, e a volte è il risultato della combinazione di diversi eventi. Può essere difficile per un trader capire esattamente cosa sta provocando lo slippage. Sebbene il commercio di criptovalute sia meno soggetto a condizioni di mercato complesse, può essere ancora difficile comprendere esattamente perché si verifichi lo slippage.

Ecco alcuni dei motivi più comuni per cui lo slippage si verifica in genere nei mercati forex:

- Volatilità del mercato: Le fluttuazioni del mercato possono rendere molto più difficile per un trader eseguire un'operazione a un determinato prezzo.
- Gap del mercato: Quando il mercato si apre, può verificarsi un gap. Questo può significare che un trader non sarà in grado di acquistare o vendere alla sua/suo valutazione.
- Prezzo di esecuzione: I trader possono stipulare accordi con i loro broker in base ai quali verranno eseguiti gli scambi.
- Liquidità del mercato: Quando c'è poca liquidità nel mercato, i merchant possono trovare molto difficile eseguire le operazioni ai prezzi previsti.

I merchant possono anche trovare che il broker limiti l'operazione a una frazione di un centesimo di centesimo di centesimo di centesimo. In genere, queste operazioni sono portate a termine con successo.

Tuttavia, se le condizioni di mercato sono volatili, lo slippage può verificarsi prima che lo scambio possa essere portato a termine. Il prezzo al quale verrà eseguita la transazione può essere diverso da quello previsto.

Può verificarsi un gap di mercato. Un gap di mercato può essere descritto come un intervallo di prezzo nel mercato. Il gap di mercato si verifica quando il mercato si apre dopo un intervallo di tempo, come dalla chiusura del giorno precedente. In genere, i gap di mercato si verificano quando si presenta un evento di mercato. Alcuni esempi sono l'annuncio di politica monetaria, un'incursione di volatilità o una pubblicazione degli utili. Quando si verifica un evento di mercato, il mercato può iniziare a muoversi molto rapidamente. Ciò può significare che i trader possono trovare difficile eseguire gli scambi. Questo è perché i prezzi possono cambiare molto velocemente.

Per questo motivo, può essere molto più probabile che si verifichi uno slippage.

Smart Contract

Livello: base

Argomento: tecnologia

Uno smart contract è un particolare programma progettato come un contratto auto-applicativo automatizzato che funziona tramite blockchain, e attiva determinate azioni dopo che sono state soddisfatte delle condizioni predeterminate.

Gli smart contract possono essere utilizzati, ad esempio, come accordi digitali che intermediano lo scambio di criptovalute (o qualsiasi altra risorsa digitale) tra due parti. Una volta fissati i termini dell'accordo, lo smart contract ne verifica l'adempimento e i beni vengono distribuiti in conformità.

Gli smart contract sono stati resi popolari dalla rete blockchain di Ethereum, ma il concetto è stato descritto per la prima volta dal crittografo americano Nick Szabo nel 1994.

Anche Bitcoin esegue smart contract grazie alle funzioni del suo linguaggio di script, anche se capacità degli smart contract Bitcoin sono ridotte alle operazioni di base, come firme digitali, timelock e hash lock, e il linguaggio utilizzato da Bitcoin viene considerato non Turing-Complete; questa limitazione del linguaggio viene considerata una caratteristica di valore perché fornisce a Bitcoin una maggiore stabilità e sicurezza.
Per l'esecuzione di smart contract più complessi su Bitcoin si ricorre a soluzioni quali Side Chain o Layer di secondo livello quali RGB, Taproot Assets Protocol

Soft fork

Livello: intermedio

Argomento: tecnologia

Il soft fork è una modifica al protocollo che consente un aggiornamento che continua a funzionare anche se alcuni nodi non aggiornano i loro software.
Poiché i vecchi nodi riconosceranno i nuovi blocchi come validi, un soft fork è retrocompatibile.
Questo tipo di fork può richiedere che sia solo la maggioranza dei miner che si aggiorni per far rispettare le nuove regole, al contrario di un hard fork che richiede che tutti i nodi si aggiornino e si accordino sulla nuova versione.
Generalmente i soft fork vengono effettuati dai miner che si aggiornano per attivare le nuove regole, in questo caso può essere definito MASF (miner-activated softfork, softfork attivato dai miner) termine poco utilizzato.
Quando l'aggiornamento per essere attivato richiede che tutti i nodi si coordinino per far rispettare le nuove regole, senza il supporto dei minatori, si chiama UASF o softfork attivato dall'utente.

Il termine softfork inizia ad essere usato nel 2012, in relazione all'introduzione del tipo di firma P2SH: la sua attivazione venne effettuata con una soglia del 55% dei miner, ma dopo che è stato attivato l'aggiornamento, il 45% dei miner che non aveva effettuato l'upgrade produsse blocchi non validi per diversi mesi dopo l'attivazione. Questo venne considerato un problema e quindi venne scelta una nuova soglia del 95%, soglia che viene attualmente considerata come necessaria e formalizzata dal BIP 9

Anche la modifica effettuata da Satoshi Nakamoto nel luglio 2010 che limitava la dimensione del blocco a 1 MB, che entrò in vigore a settembre 2010, viene considerata un softfork perché all'epoca non c'erano ancora così tante transazioni da riempire un blocco di 1 MB: impostando tale limite venivano ristrette le regole, e i nodi non avevano necessità di aggiornare il software. Un ipotetico incremento del limite avrebbe invece richiesto un aggiornamento del software e sarebbe quindi stato un hard fork.

SOPR

Acronimo di: Spent Output Profit Ratio

Livello: avanzato

Argomento: economia

Spent Output Profit Ratio è un indicatore chiave per monitorare il comportamento di spesa on-chain e l'attuale sentiment del mercato. Fornisce informazioni sul sentiment del mercato, sulla redditività e sulle perdite rilevate in un particolare lasso di tempo. Riflette il grado di profitto realizzato per tutte le monete spostate on-chain. Il SOPR viene misurato considerando solo le monete spostate

nella scala temporale considerata (giornaliera, oraria ecc.) e prendendo il rapporto tra il valore fiat al momento della creazione dell'UTXO e il valore fiat quando l'UTXO viene speso.

spam

Livello: base

Argomento: tecnologia

Il termine spam nasce riferito all'inivo massivo tramite email di messaggi pubblicitari indesiderati o non richiesti, generalmente di carattere commerciale.

Il termine si è esteso ad altri casi.

Il concetto di spam in relazione a Bitcoin si amplia oltre la sua originaria associazione con l'invio massivo di messaggi pubblicitari via email. Nel contesto delle criptovalute, il termine è adottato per descrivere contenuti messaggi arbitrari che vengono immagazzinati sulla blockchain di Bitcoin attraverso diverse modalità.

La definizione di cosa costituisca spam in questo contesto è oggetto di controversie e variazioni interpretative. A differenza del classico spam via email, dove la natura indesiderata e commerciale dei messaggi è generalmente chiara, nel contesto di Bitcoin la linea di demarcazione è più sfumata. Un esempio emblematico è rappresentato dalle Inscription degli Ordinal, una pratica che suscita opinioni divergenti nella comunità bitcoin.

Alcuni considerano le Inscription degli Ordinal come spam, sostenendo che rappresentano un utilizzo non conforme della blockchain, poiché appesantiscono la dimensione della blockchain con dati non legati direttamente alla trasmissione di valore. D'altra parte, vi sono coloro che vedono questa pratica come un'operazione legittima e creativa, sfruttando la natura aperta e decentralizzata di Bitcoin per immagazzinare informazioni, come ad esempio firme digitali, informazioni per la notarizzazione di contenuti esterni a Bitcoin, messaggi simbolici, NFT, token.

Hashcash C'è un altro collegamento tra Bitcoin e lo spam, tramite Hashcash. Hashcash è un sistema proposto da Adam Back per limitare lo spam attraverso l'uso della proof-of-work.
Nel whitepaper Bitcoin in relazione alla Proof-of-Work, viene indicato: "*Per implementare un server di marcatura temporale distribuito su base peer-to-peer, avremo bisogno di usare un sistema simile a quello di Hashcash di Adam Back*"

Sparse Merkle tree

Livello: avanzato

Argomento: tecnologia

Uno Sparse Merkle Tree, SMT, è come un Merkle Tree standard, eccetto che i dati contenuti sono indicizzati, e ogni datapoint è posizionato alla foglia che corrisponde all'indice di quel datapoint.

Analogamente al Merkle tree standard, possiamo usare una Merkle proof per dimostrare che A fa parte di questo albero, ma in più offre la possibilità di effettuare una efficiente prova di non-inclusione ovvero è possibile dimostrare facilmente se uno o più dati specifici non esistono all'interno del Merkle Tree.

Uno Sparse Merkle Tree è un archivio chiave-valore autenticato, il che significa che la chiave, o la posizione, di una foglia e il contenuto della foglia sono legati l'uno all'altro.

Per ottenere questa proprietà, il contenuto della foglia viene sottoposto a hash e viene creato un merkle tree in cui la posizione della foglia corrisponde alla bitmap dell'hash digest.

Per forza di cose, questo richiede un albero di 256 livelli e 2^256 foglie. La generazione dell'albero è efficiente, nonostante le dimensioni apparentemente elevate, perché la stragrande maggioranza dei rami contiene foglie vuote e può essere rappresentata con hash nulli.

Nei Sparse Merkle Tree, ogni foglia può essere descritta come una guida verso se stessa attraverso una mappa espressa in forma binaria. La mappa è l'albero di Sparse Merkle stesso e la guida è rappresentata da istruzioni che indicano se girare a sinistra o a destra a ogni bivio. La nona foglia di un albero di Sparke Merkle grande 2^4, ad esempio, è espressa in forma binaria come 1001, il che significa che troviamo la foglia appropriata girando a sinistra, poi a destra, a destra e infine a sinistra.

Poiché ogni elemento ha una posizione predeterminata, l'hash della radice dell'albero non dipende dall'ordine di inserimento degli elementi.

Speedy Trial

Livello: avanzato

Argomento: politica

Speedy Trial è una modalità di attivazione di un soft fork bitcoin. È stato il modo in cui Taproot è stato attivato con successo. È stata una scelta molto controversa dei meccanismi di attivazione. Speedy Trial funziona come l'attivazione di un'implementazione BIP9, tranne per il fatto che la finestra di attivazione è molto più breve e la soglia di segnalazione è la stessa di BIP8 (90%). Parte della motivazione per l'utilizzo di Speedy Trial è stato che se qualcosa con consenso non si attivava, un'implementazione BIP8 LOT=True poteva essere rilasciata in seguito. In molti hanno visto Speedy Trial come un passo indietro in termini di perfezionamento dei meccanismi di attivazione delle funzionalità.

Spent Output

Output speso

Livello: intermedio

Argomento: tecnologia

A uno spent output, a volte definito come coin moved o UTXO destruction, è un UTXO distrutto dal proprietario trasmettendo una transazione di spesa alla rete che viene successivamente confermata dai minatori/validatori.

SPHINX Mix Format

Livello: avanzato

Argomento: tecnologia

Una particolare tecnica di onion routing utilizzata nella rete Lightning e inventata da George Danezis e Ian Goldberg nel 2009. Con il formato SPHINX Mix, ogni messaggio del pacchetto onion viene imbottito con alcuni dati casuali, in modo che nessun singolo hop possa stimare la distanza percorsa lungo il percorso. Mentre la privacy del mittente e del destinatario del pagamento è protetta, ogni nodo è comunque in grado di restituire un messaggio di errore lungo il percorso al mittente del messaggio.

splicing

Livello: avanzato

Argomento: tecnologia

Lo splicing è una funzionalità avanzata introdotta su Lightning Network, per superare una delle inziali limitazioni nella modifica della liquidità dei canale Lightning.

Senza lo splicing, se una delle parti volesse aggiungere o prelevare fondi, dovrebbe chiudere il canale di pagamento attuale e aprirne uno nuovo, il che potrebbe essere inefficiente e costoso a causa delle commissioni di transazione di Bitcoin.

Lo splicing consente di modificare la liquidità di un canale senza la necessità di chiuderlo, migliorando l'esperienza utente e aiutando i nodi di instradamento a riallocare la liquidità in modo più efficiente.

Esistono due tipi di splicing:

- **Splice-in** che significa aggiungere fondi a un canale. Per farlo, i partecipanti creano congiuntamente una nuova transazione che spende l'output della Funding Transaction originale e aggiunge ulteriori fondi. Questa nuova transazione diventa la nuova Funding Transaction per il canale e la capacità del canale viene aumentata di conseguenza

- **Splice-out** che consente di ritirare fondi da un canale. I partecipanti creano una nuova transazione che spende l'output della Funding Transaction originale e invia parte dei fondi a un altro indirizzo on-chain (ritirandoli di fatto dal canale). I fondi rimanenti diventano la nuova Funding Transaction per il canale e la capacità del canale viene ridotta di conseguenza.

L'operazione di splicing richiede una transazione on-chain, ma non è necessario che il canale venga chiuso e riaperto, e la cronologia delle transazioni off-chain del canale viene preservata.

Lo splicing funziona firmando una nuova transazione multi-firma 2-su-2 per bloccare i fondi per il canale Lightning.

Lo splicing è stato proposto da Dusty Daemon, uno sviluppatore principale di Lightning, nel 2021 e modifica i BOLT 2, 7 e 9. Dusty ha effettuato uno splice sulla mainnet e diverse implementazioni del protocollo Lightning stanno lavorando allo splicing. Lo splicing ha il potenziale per aumentare la privacy di Bitcoin, poiché la transazione di splice può essere utilizzata come coinjoin.

Lo splicing è diverso dai submarine swap (come quelli implementati da Lightning Loop), in cui i fondi vengono trasferiti tra gli utenti in cambio di transazioni onchain: nei submarine swap, il saldo complessivo del canale rimane lo stesso; nello splicing, il saldo complessivo del canale cambia.

SPV

Acronimo di: Simplified Payment Verification

Verifica semplificata dei pagamenti

Livello: avanzato

Argomento: tecnologia

Gli SPV sono una modalità descritta nel white paper Bitcoin di Satoshi Nakamoto, che consente di usare i Bitcoin senza dover eseguire un full node per verificare le transazioni.

Come impostazione predefinita, alla ricezione di una nuova transazione un nodo deve convalidarla: in particolare, verificare che nessuno degli input della transazione sia stato speso in precedenza. Per effettuare questo controllo il nodo deve accedere alla blockchain. Ogni utente che non si fida dei suoi vicini di rete, dovrebbe tenere una copia locale completa della blockchain, in modo che ogni input possa essere verificato.

Nel whitepaper viene indicato che è possibile verificare i pagamenti bitcoin senza eseguire un nodo di rete completo. E questo è chiamato verifica di pagamento semplificata o SPV. Un utente o il portafoglio bitcoin SPV dell'utente ha solo bisogno di una copia dei Block header della catena più lunga, che sono disponibili interrogando i nodi di rete fino a quando non è evidente che la catena più lunga

è stata ottenuta. Poi, il portafoglio che usa il client SPV ottiene il ramo Merkle che collega la transazione al suo blocco. Collegare la transazione a un posto nella catena attiva dimostra che un nodo della rete l'ha accettata, e i blocchi aggiunti dopo di essa stabiliscono ulteriormente la conferma.

SSS

Acronimo di: Shamir's Secret Sharing

Livello: avanzato

Argomento: tecnologia

Shamir's Secret Sharing, abbreviato SSS, la condivisione Shamir del segreto, è un efficiente algoritmo di condivisione di un segreto per distribuire informazioni private (il *secret*) in modo tale che nessun individuo possieda informazioni intelligibili sul segreto.

Per ottenere questo risultato, il segreto viene convertito in parti (*share*) dalle quali il segreto può essere ricomposto quando un numero sufficiente di azioni viene combinato, ma non altrimenti.

L'SSS ha l'insolita proprietà della sicurezza teorica dell'informazione, ovvero un avversario senza un numero sufficiente di azioni non può ricostruire il segreto nemmeno con tempo e capacità di calcolo infiniti.

Una specifica SSS standard per il backup wallet di criptovalute è stata ampiamente implementata, chiamata Shamir Backup.

Il Shamir's Secret Sharing è un metodo di crittografia a chiave pubblica che consente di suddividere una chiave segreta in un numero di parti, dette share, in modo tale che sia possibile ricostruire la chiave solo se si dispone di un numero sufficiente di share, threshold. Questo metodo è stato sviluppato da Adi Shamir, un matematico e informatico israeliano.

Il suo funzionamento nella sua forma generica e teorica è il seguente: si sceglie il numero di share che si desidera ottenere e il numero minimo di share necessarie per ricostruire la chiave segreta. Quindi, si seleziona una curva ellittica e si utilizza un algoritmo di crittografia a chiave pubblica per generare una coppia di chiavi pubblica e privata. La chiave privata viene quindi suddivisa in tante share quante ne sono state specificate in precedenza, utilizzando un polinomio di grado inferiore al numero di share. Ogni condivisione contiene un indice univoco e un valore, che può essere utilizzato per ricostruire la chiave privata se si dispone di un numero sufficiente di share.

Il Shamir's Secret Sharing è un metodo molto utile per proteggere le chiavi segrete, poiché permette di distribuire le share in modo tale che nessun singolo individuo possa ricostruire la chiave segreta. Inoltre, il metodo è resistente alla compromissione di una o anche di molte share, poiché è necessario disporre di un numero minimo di share per ricostruire la chiave segreta.

Stablecoin

Livello: base

Argomento: finanza

Una Stable coin è un token il cui valore è peggato (ancorato) a un'altra fonte di valore, tipicamente una valuta fiat. Ad esempio, per una stable coin peggata al dollaro il valore dovrebbe essere uguale a $1.

Le stablecoin sono comunemente utilizzate per facilitare il trading di criptovalute e per il trasferimento dentro e fuori da un exchange che avviene in tempi molto veloci rispetto ai bonifici bancari che possono richiedere giorni.

Per poter mantenere questo rapporto fisso 1 a 1, le stablecoin usano diverse strategie, anche in funzione della tipologia di stablecoin, quali:

- **Collateralizzate**: il loro valore è garantito da un collaterale, che può essere una valuta fiat, una criptovaluta o un altro tipo di asset
- **Non collateralizzate**, quali le stablecoin algoritmiche
- Basate su posizioni short in perpetual swap di una particolare cripto, spesso Bitcoin

Possiamo suddividere le stablecoin 2 tipologie: centralizzate e decentralizzate. Le stablecoin centralizzate sono create e governate da organizzazioni centralizzate, come società, banche o governi.
Alcuni esempi di stablecoin centralizzate gestite da società tra le più popolari sono Tether (USDT), USD coin (USDC), Gemini USD (GUSD).
Le stablecoin decentralizzate sono governate dal consenso degli utenti che partecipano alla community della stablecoin, anche se a volte questa presunta decentralizzazione ha dei punti deboli più o meno evidenti o trasparenti che trasferiscono il controllo ad alcuni soggetti quali i fondatori.

La strategia più semplice per garantire l'ancoraggio dovrebbe essere quella di effettuare l'emissione della criptovaluta avendo una riserva equivalente dell'asset al quale sono ancorate, questa riserva viene definita Collateral (o garanzia) e l'operazione collateralizzazione.
Le stablecoin con collaterale Fiat sono agganciate al valore della valuta fiat, spesso il dollaro USA. Il collaterale Fiat rimane in riserva presso l'emittente centrale e deve riflettere il numero di stablecoin corrispondenti in circolazione.
È importante notare, tuttavia, che non tutte le stablecoin garantite da fiat sono uguali. Ad esempio, alcuni emittenti di stablecoin sono più trasparenti riguardo alla regolamentazione e al luogo in cui sono detenuti i fondi a sostegno delle loro stablecoin. Alcuni emittenti rilasciano relazioni di revisione di terze parti per dimostrare pubblicamente il loro peg 1:1. Se un emittente detiene 1.000 dollari di riserva, possono circolare solo 1.000 stablecoin del valore di 1 dollaro ciascuno. Il collaterale fiat non è bloccato negli smart contract, quindi esiste fuori dalla chain, tradizionalmente in un conto bancario. Gli operatori possono scambiare le stablecoin garantite da fiat con altri asset crittografici

o riscattarle con fiat tradizionali. Ci sono stablecoin che sono sostenute da materie prime come immobili, oro, argento e altri metalli preziosi Ad esempio, Kitco Gold è sostenuto dalle riserve d'oro della società e il token stesso è basato sull'ecosistema blockchain ERC-20 su blockchain Ethereum.

Non sempre esiste questa riserva, e in generale questo ancoraggio viene effettuato attraverso la contrazione o la diluizione dell'offerta totale dei token della stable coin. Le variazioni nell'offerta di token modificheranno il prezzo relativo di ciascun token, fino a raggiungere il peg desiderato. Le stablecoin come USDT e DAI di MakerDAO vengono coniate e bruciate a seconda dei casi, con i token appena coniati che ricevono un supporto collaterale sotto forma di altri asset digitali o criptovalute. Con DAI l'utente può bloccare una certa quantità di criptovalute, come gli Ether, come garanzia per prendere in prestito DAI, che è peggato al dollaro USA. In pratica è necessario depositare 1.000 dollari in ETH per acquistare 500 dollari di stablecoin DAI.

Le stablecoin algoritmiche mantengono il loro ancoraggio attraverso una combinazione di collateralizzazione e l'utilizzo di complessi algoritmi di contratti intelligenti che contraggono ed espandono l'offerta in base a vari fattori di mercato; il crollo a maggio 2022 della stable coin UST (Terra USD) e dell'ecosistema Terra collegato ha mostrato i rischi e la fragilità della stablecoin algoritmica.

Stacks

Livello: avanzato

Argomento: tecnologia

Stacks è una piattaforma di blockchain che opera come livello 2 su Bitcoin, consentendo la creazione e l'esecuzione di smart contract sulla rete Bitcoin senza la necessità di apportare modifiche al protocollo di Bitcoin stesso. Invece, utilizza la blockchain di Bitcoin come livello di sicurezza e affidabilità, consentendo agli sviluppatori di creare contratti intelligenti utilizzando il linguaggio di programmazione Clarity.

Stacks utilizza un processo chiamato "impilamento" (stack) per collegare i dati di livello applicazione ai blocchi Bitcoin. Questo rende le applicazioni Stacks immutabili, trasparenti e sicure.

Per impilare, un utente deve depositare Bitcoin in un contratto intelligente Stacks. Il contratto intelligente quindi utilizza questi Bitcoin per acquistare spazio sul blocco Bitcoin. I dati di livello applicazione vengono quindi archiviati nello spazio acquistato. Quando un nuovo blocco viene creato su Bitcoin, i dati di livello applicazione vengono archiviati anche nel blocco Bitcoin.

Questo processo consente agli sviluppatori di creare applicazioni decentralizzate che sono ancora protette dalla sicurezza di Bitcoin. Le applicazioni Stacks possono essere utilizzate per una varietà di scopi, tra cui:

- Creazione di contratti intelligenti

- Creazione di applicazioni decentralizzate
- Creazione di mercati decentralizzati
- Creazione di sistemi di pagamento decentralizzati

Stacks è ancora in fase di sviluppo, ma ha il potenziale per rivoluzionare il modo in cui creiamo e utilizziamo le applicazioni decentralizzate.

Ecco alcuni vantaggi di Stacks:

- Sicurezza: Stacks utilizza la sicurezza di Bitcoin, che è una delle blockchain più sicure al mondo.
- Trasparenza: tutte le transazioni su Stacks sono pubbliche e verificabili.
- Decentralizzazione: Stacks è una rete decentralizzata, il che significa che non è controllata da nessuna entità centrale.
- Scalabilità: Stacks è progettato per essere scalabile, il che significa che può gestire un gran numero di transazioni.

Stake / Staking

Livello: intermedio

Argomento: tecnologia

Lo staking è l'atto di bloccare le criptovalute per ricevere ricompense, e quindi avere un reddito passivo.

Lo staking si riferisce all'attività di impegnare o bloccare un quantitativo delle proprie criptovalute al fine di guadagnare con servizi con protocollo PoS, o per contribuire a sistemi di finanza decentralizzata DeFi. Le barriere allo staking sono piuttosto alte e gli utenti normalmente devono prima detenere un grosso quantitativo di una particolare criptovaluta se fatte individualmente. Nel caso dei sistemi DeFi, gli utenti bloccano le loro criptovalute nel loro wallet ma danno il permesso a una terza parte, spesso un exchange, di effettuare l'exchange delle proprie criptovalute su progetti DeFi che offrono interessi. Alcuni exchange, ad esempio Binance e Coinbase, offrono la possibilità ai propri clienti di partecipare allo staking con una parte dei propri depositi anche con importi non alti.

Staking Derivative

Livello: intermedio

Argomento: finanza

Uno staking derivative (derivato) è uno strumento finanziario che viene tipicamente impiegato all'interno di specifici tipi di protocolli blockchain di finanza decentralizzata (DeFi). I derivati di staking sfruttano lo staking o il deposito di asset in un protocollo blockchain per accumulare regolari ricompense finanziarie, in forma derivata, di solito attraverso un protocollo blockchain Proof-of-Stake (PoS). Ai derivati di staking viene spesso assegnato un prefisso davanti al nome

del token tradizionale, come “cTokens” che rappresentano altri asset come ETH (sotto forma di cETH) all’interno della blockchain Compound.

Staking Pool

Livello: intermedio

Argomento: tecnologia

Uno staking pool consente a più parti interessate (stakeholder) di partecipare in modo collettivo combinando le proprie risorse in modo da aumentare le probabilità di ottere la ricompensa derivante dallo staking.

In altre parole, uniscono il loro potere di staking quindi hanno una maggiore probabilità di guadagnare i premi o fee. L’idea generale del modello di staking pool è abbastanza simile al tradizionale mining pool, che prevede il raggruppamento del tasso di hash in una blockchain Proof of Work (PoW). Tuttavia, la configurazione dello staking pool è disponibile solo su blockchain che utilizzano il modello Proof of Stake (PoS) o, in sistemi non POS, tramite funzionalità di progettazione del protocollo. In genere, uno staking pool è gestito da un operatore di pool e gli stakeholder che decidono di aderire al pool devono bloccare i propri token o coin in uno specifico indirizzo blockchain (o wallet). Mentre alcuni pool richiedono agli utenti di puntare le loro coin con una terza parte, ci sono molte altre alternative che consentono alle parti interessate di contribuire con la propria dotazione di staking mentre conservano le loro coin in un portafoglio personale.

Gli staking pool forniscono ricompense di staking più prevedibili e frequenti. Oltre a ciò, consentono alle parti interessate di ottenere un reddito passivo senza doversi preoccupare dell’implementazione tecnica e della manutenzione dell’impostazione e dell’esecuzione di un nodo di convalida.

Stamps

Livello: avanzato

Argomento: tecnologia

I Bitcoin Stamps, termine traducibile in italiano in “francobolli”, sono un nuovo tipo di NFT sulla blockchain bitcoin, proposto nel 2023 dallo sviluppatore noto con lo pseudonimo Mike In Space.

I Bitcoin Stamps, o token SRC-20, vengono creati secondo un apposito protocollo. STAMPS è l’acronimo di Secure Tradeable Art Maintained Securely.

Il protocollo incorpora i dati dell’immagine negli UTXO invece di memorizzarli nei dati dei witness che possono essere “prunabili”, rispetto a quanto succede per altri tipi di NFT quali le Inscripition

Attualmente ci sono 2 protocolli utilizzati in Bitcoin Stamps: SRC-20 per i token fungibili, e SRC-721 per gli NFT.

SRC-20 SRC-20 è ispirato da BRC-20.

Le immagini dei Bitcoin Stamps possono essere di tre tipi: SVG, PNG e GIF. Il protocollo Bitcoin STAMPS converte un'immagine in un formato chiamato base64 che consente di rappresentare l'immagine come una stringa di caratteri. La stringa viene aggiunta alla chiave di descrizione di una transazione Bitcoin e trasmessa alla blockchain dall'indirizzo che detiene il saldo SRC-20.

Inizialmente, durante la fase di prova concettuale, il protocollo utilizzava Counterparty per trasmettere le transazioni SRC-20 alla blockchain. A partire dal blocco 796.000, gli utenti non possono più utilizzare Counterparty per generare token SRC-20. Se lo fanno, la transazione SRC sarà considerata non valida.

Codificando direttamente le transazioni SRC-20 sulla blockchain di Bitcoin anziché utilizzare Counterparty, sono stati ridotti i costi delle transazioni. Tuttavia, le commissioni di transazione per la produzione di un token SRC-20 possono ancora essere superiori a quelle della registrazione di una Inscription e per questo motivo, viene suggerito agli utenti di incorporare immagini con risoluzioni di 24 per 24 pixel.

I Bitcoin Stamps sono numerati cronologicamente, con uno schema di numerazione che parte da zero e continua indefinitamente.

SRC-721 SRC-721 è una specifica che si concentra sulla possibilità di creare NFT componibili ad alta risoluzione a un costo più accessibile. Affronta la necessità di un modo economico per coniare questi NFT. Il protocollo consente di memorizzare collezioni d'arte come livelli utilizzando il protocollo STAMPS, riducendo le dimensioni del file mediante l'utilizzo di tecniche come le tavolozze dei colori indicizzate per ciascun livello. Richiamando i dati on-chain, viene utilizzato un piccolo file JSON per creare un NFT composto da questi livelli, risultando in prodotti finali visivamente accattivanti e di alta qualità.

Per garantire la stabilità dei riferimenti agli asset di fronte a modifiche del protocollo, la specifica SRC-721 utilizza gli ID degli asset counterparty. Ciò aiuta a proteggere le collezioni SRC-721 implementate da eventuali impatti derivanti da futuri cambiamenti al protocollo Stamps.

La specifica delinea vari tipi di transazione, tra cui deployment, reveal, minting per collezioni e oggetti singoli, e transfer/use per token SRC-721. Vengono specificati i requisiti per i token SRC-721, inclusi i caratteri consentiti, la lunghezza e le limitazioni per campi come il numero massimo di mint e i limiti per ciascuna mint.

Stateless invoice

Livello: avanzato

Argomento: tecnologia

Le Stateless invoice sono Lightning Invoice la cui preimage di pagamento è generata in modo deterministico dai metadati di pagamento.

Ciò consente al destinatario di un pagamento di non memorizzare alcun dato sulla invoice fino a quando il mittente non invia una copia dei metadati insieme al pagamento.

STO

Acronimo di: Security Token Offering

Livello: intermedio

Argomento: finanza

È una forma di ICO nella quale i token sono di tipo Security

Stop loss

Livello: intermedio

Argomento: finanza

Un metodo di trading per limitare le perdite. È un ordine effettuato su una posizione aperta che impone la chiusura della stessa ad un prezzo predefinito, che risulta meno favorevole rispetto al prezzo di mercato corrente. Lo strumento dello stop loss è molto utile per definire un limite massimo di perdite possibili che si è disposti ad affrontare per una determinata posizione aperta. L'opposto del take profit.

Store of value

Bene rifugio

Livello: base

Argomento: economia

Uno Store of value, noto anche come Bene rifugio, è un concetto economico che identifica un bene, una merce o una valuta in grado di essere conservato, recuperato e scambiato nel corso del tempo senza subire una degradazione del suo valore o del suo prezzo.

Caratteristiche di uno Store of value:

- **Durabilità**: il bene deve essere resistente alla corrosione, all'usura e al deterioramento.
- **Scarsità**: il bene deve essere limitato in quantità o difficilmente reperibile.
- **Divisibilità**: il bene deve essere facilmente suddivisibile in unità più piccole senza perdere valore.

- **Trasportabilità**: il bene deve essere facilmente trasferibile da un luogo all'altro senza costi eccessivi.
- **Accettazione**: il bene deve essere riconosciuto e richiesto da un ampio numero di persone o istituzioni, garantendo la sua fungibilità e liquidità sul mercato.

Storicamente, l'oro è stato considerato il Bene rifugio per eccellenza, grazie alle sue proprietà fisiche, durabilità, scarsità e accettazione universale.

Bitcoin, sebbene sia noto per la sua volatilità, viene paragonato all'Oro digitale per alcune delle sue caratteristiche, che potrebbero renderlo un Bene rifugio digitale in misura simile, se non superiore, rispetto all'oro tradizionale:

- **Durabilità**: Mentre l'oro è fisicamente resistente al degrado, Bitcoin, essendo una moneta digitale, mantiene costantemente la sua quantità e il suo valore senza subire ossidazione o deterioramento, 1 Bitcoin sarà sempre 1 Bitcoin
- **Scarsità**: Bitcoin presenta un vantaggio rispetto all'oro in termini di assoluta scarsità. Il limite massimo di Bitcoin è noto e inalterabile, a differenza dell'oro, che potrebbe essere soggetto a nuove scoperte di riserve o a innovazioni tecnologiche che ne influenzano la disponibilità.
- **Divisibilità**: l'oro ha una buona divisibilità, poiché può essere fuso e coniato in monete, lingotti o gioielli di varie dimensioni e pesi. Tuttavia, la divisibilità dell'oro richiede costi e risorse aggiuntivi per la lavorazione e la certificazione. Bitcoin ha una eccellente divisibilità, può essere suddiviso in unità molto piccole chiamate satoshi o sat, pari a un centomilionesimo di Bitcoin; con Lightning Network viene utilizza una unità di conto più piccola del satoshi, chiamata millisatoshi, che equivale a un millesimo di satoshi. Questo significa che con Lightning Network è possibile frazionare ulteriormente un satoshi e trasferire quantità molto piccole di valore. Tuttavia, queste quantità non sono riflettute sulla block chain di Bitcoin in caso di chiusura dei canali di pagamento. Infatti, quando un canale viene chiuso, eventuali importi inferiori a un satoshi detenuti da ciascuna parte vengono arrotondati. Quindi, in termini di frazionabilità, Lightning Network permette di aumentare la divisibilità del Bitcoin rispetto all'oro, ma solo a livello off-chain e senza garanzie on-chain
- **Trasportabilità**: l'oro è un bene materiale che ha una certa massa e volume e che quindi occupa uno spazio fisico. Per spostare l'oro da un luogo all'altro, bisogna trasportarlo con mezzi adeguati, che comportano dei costi e dei rischi. Bitcoin invece è un bene immateriale che non ha massa né volume e che quindi non occupa uno spazio fisico, non si trova su un dispositivo o su un software specifico, ma è registrato sulla blockchain, che è una sorta di libro contabile distribuito e condiviso tra tutti i nodi della rete e quindi non ha bisogno di essere trasportato: si trova contemporaneamente in qualunque parte del mondo; il suo possesso può essere trasferito tramite una transazione.
- **Accettazione**: In questo ambito, l'oro ha ancora un vantaggio significa-

tivo rispetto a Bitcoin. L'oro gode di una maggiore fiducia e reputazione tra le persone e le istituzioni, mentre Bitcoin sta ancora guadagnando accettazione e fiducia nel contesto economico e finanziario globale.

Va notato che, nonostante la volatilità, nel lungo periodo Bitcoin ha dimostrato una tendenza di apprezzamento.

Stratum

Livello: avanzato

Argomento: tecnologia

Stratum, o Stratum-mining, è un protocollo per il mining in pool.

È un protocollo di comunicazione utilizzato dai miner e dalle mining pool per richiedere i dati da elaborare per il mining e per trasmettere i risultati delle elaborazioni.

Il protocollo è nato per sostituire il precedente protocollo getwork obsoleto alla fine del 2012. Le specifiche del servizio sono state inizialmente annunciate nel sito web di Slush pool, e successivamente una documentazione è stata fornita da BTC Guild.

Nella prima versione di Stratum, la mining pool fornisce ai miner un block template, ovvero una struttura di blocco già impostata con un insieme di transazioni.
I miner fanno il lavoro di hashing, trovare il nonce corretto per risolvere il blocco, non hanno controllo diretto sulle transazioni incluse nel blocco proposto. La pool può quindi censurare delle transazioni, ma deve farlo di nascosto: se i miner si accorgono che una pool sta censurando transazioni per motivi politici o arbitrari, si spostano su un'altra pool più redditizia.

Ci sono dei precedenti noti:

- – Marathon nel 2021, aveva annunciato l'intenzione di estrarre "blocchi conformi alle normative", escludendo intenzionalmente le transazioni provenienti da indirizzi sanzionati o associati ad attività illecite, ma a seguito della reazione della comunità Bitcoin ha abbandonato questa ipotesi
- – F2Pool nel 2023 è stato accusato di non aver convalidato sei transazioni provenienti da indirizzi segnalati dall'OFAC. Il cofondatore di F2Pool, Chun Wang, ha inizialmente difeso questa scelta, per decidere poi di abbandonare la pratica fino a quando la comunità non raggiungerà un consenso più ampio
- – Ocean nel 2023 con l'intenzione di filtrare le transazioni considerate spam quali quelle relative agli Ordinal, è stata accusata da Samourai Wallet di censurare le transazioni CoinJoin

Anche qui funziona il gioco degli incentivi, e infatti le mining pool sono soggetti sotto scrutinio da parte dei miner.

Stratum v2 La nuova versione è la V2 che dovrebbe risolvere diversi problemi tra cui comunicazione crittografata, autenticazione e un maggior trasferimento ai miner rispetto al pool per le decisioni sulla composizione dei blocchi finali per selezionare e ordinare le transazioni, con positivi impatti sull'ecosistema Bitcoin.
Con Stratum V1 è la pool che sceglie le transazioni da inserire nel blocco, non il miner. Stratum V2 introduce tre nuovi sottoprotocolli che consentono ai miner di selezionare i propri set di transazioni attraverso un processo di negoziazione con i pool, migliorando la decentralizzazione.
Con Stratum v2, il miner dichiara le transazioni alla pool, che può quindi scegliere di accettarle o rifiutarle, per questo motivo tale funzionalità che inizialmente è stata conosciuta come Job Negotiator è stata rinominata Job Declarator.
Nei casi in cui una pool accetta le transazioni dichiarate, queste vengono successivamente propagate alla rete bitcoin. Se invece la pool rifiuta le transazioni (e quindi sta facendo censura), il miner cercherà automaticamente una pool alternativa. Se anche questa pool rifiuta di includere le transazioni, il miner continuerà a passare ad un'altra pool, ricorrendo infine al solo mining.

A novembre 2023, la mining pool Demand ha lanciato la prima mining pool con l'utilizzo di Stratum V2.

A marzo 2024 viene rilasciata la SRI (Stratum Reference Implementation) 1.0.0 di Stratum V2.

Submarine Swap

Livello: avanzato

Argomento: tecnologia

Non è possibile inviare direttamente Bitcoin da un canale lightning a un normale indirizzo on-chain. I submarine swap, che si basano sugli stessi principi dei normali atomic swap, forniscono una soluzione a questo problema.

I submarine swap sono swap atomici da on-chain a off-chain (e viceversa) di criptovalute. Sono progettati per facilitare il trasferimento dalla blockchain Bitcoin ad un canale LN (Lightning Network). A differenza degli atomic swap, nei quali Lightning Network deve essere abilitato su entrambe le criptovalute che partecipano allo swap, con submarine swap è sufficiente che Lightning sia abilitato su un solo lato. I submarine swap sono realizzabili anche tra diverse blockchain.

Si basano su un tipo specifico di smart contract Bitcoin chiamato HTLC, Hash Time-Locked Contracts. Poiché gli HTLC possono includere transazioni sia on-chain che off-chain, gli HTLC possono essere utilizzati anche per i pagamenti ed

è il costrutto principale che consente il trasferimento di denaro tramite Lightning Network. Gli HTLC possono anche essere sfruttati tra un mittente on-chain e un ricevente off-chain e viceversa, e questi sono submarine swap.

Lo smart contract per il submarine swap è chiamato swap provider. Può essere gestito da un servizio di terze parti ma è uno smart contract sulla blockchain. I submarine possono essere utilizzati per:

- Pagare in modo trustless uno swap provider in una rete per eseguire un pagamento sull'altra rete
- Pagare in modo trustless uno swap provider in una rete per trasferire coin sull'altra rete
- Pagare in modo trustless uno swap provider per riequilibrare i canali Lightning

Perché sono necessari i submarine swap? Il problema principale dell'indirizzo del submarine swap è che le transazioni tra indirizzi Bitcoin on-chain e indirizzi LN off-chain non sono direttamente compatibili. Non si può inviare facilmente una transazione Lightning a qualcuno che non usa il Lightning o viceversa. Questa separazione dei livelli crea una barriera di transazione tra la blockchain Bitcoin e la LN off-chain. Un'ulteriore limitazione dell'attuale implementazione di LN è che la configurazione di un canale LN richiede una transazione on-chain (e una fee successiva) e un importo precompilato di BTC inviato al canale. Una volta esaurita la fornitura di BTC nel canale, non esiste alcun metodo per ricaricare il canale e per continuare a utilizzare è necessario aprire un altro canale. Sebbene le transazioni sostanzialmente illimitate possano essere inviate all'interno di un canale LN purché nel canale siano presenti BTC sufficienti. La gestione dei canali costa più in commissioni di transazione sulla chain e come complessità, rendendo scomodo e inefficiente l'apertura ripetuta di più canali.

In che modo gli submarine swap risolvono il problema I submarine swap risolvono questo problema consentendo ricaricare i canali LN tramite un trasferimento on-chain dalla blockchain di Bitcoin al canale LN off-chain. I submarine swap sono ispirati agli atomic swap, quindi hanno un funzionamento simile. I submarine swap e atomici utilizzano un intermediario trustless per il trasferimento di token tra blockchain o intra-chain (ad esempio, Bitcoin on-chain to off-chain LN). I submarine swap sfruttano gli HTLC contract in cui il destinatario di una transazione deve riconoscere di aver ricevuto il pagamento prima di una scadenza specifica fornendo una prova crittografica del pagamento. In caso contrario, il destinatario perde la possibilità di richiedere i token e vengono restituiti al pagatore.

Supply

Livello: intermedio

Argomento: economia

Traducibile in Offerta o Fornitura, ne esistono di 3 tipi a seconda di ciò che esprime:

- Circulating supply (offerta circolante): fornisce la più appropriata approssimazione sul numero di token che circolano nel mercato e nelle mani del pubblico in generale:
  - La Circulating Supply rappresenta la quantità di una criptovaluta che è attualmente disponibile sul mercato e in circolazione.
  - Questa cifra tiene conto di tutte le monete o token che sono state estratte o emesse e che sono disponibili per il trading o l'uso.
  - Gli investitori spesso usano la Circulating Supply per calcolare la capitalizzazione di mercato di una criptovaluta (Prezzo attuale x Circulating Supply).
- Total supply (offerta totale) : quantità totale di monete o token esistenti al momento:
  - La Total Supply rappresenta l'intera quantità di una criptovaluta che è stata creata o emessa finora, comprese le monete o i token che non sono attualmente in circolazione.
  - Questa cifra include le monete o i token che potrebbero essere bloccati, inattivi o riservati per sviluppatori o altri scopi.
  - La Total Supply può essere utile per valutare il potenziale futuro dell'offerta di una criptovaluta. Max Supply (offerta massima):
- La Max Supply: fornisce la più appropriata approssimazione sulla quantità massima di token raggiungibile in quel determinato network rappresenta la quantità massima di una criptovaluta che potrà mai essere creata o emessa.
  - Questo valore è spesso fissato nel codice o nella documentazione della criptovaluta e rappresenta il limite massimo dell'offerta.
  - La Max Supply è importante perché stabilisce un tetto massimo al numero di monete o token che potranno mai esistere. Ad esempio, il Bitcoin ha una Max Supply di 21 milioni, il che significa che non ci saranno mai più di 21 milioni di Bitcoin in circolazione.

In sintesi, la Circulating Supply si riferisce alle monete o ai token attualmente in circolazione, la Total Supply rappresenta l'intera offerta finora creata, e la Max Supply è il limite massimo dell'offerta che non sarà mai superato. Questi concetti sono importanti per comprendere l'offerta di una criptovaluta e la sua capitalizzazione di mercato.

Support

Supporto

Livello: base

Argomento: finanza

Il supporto è una specie di muro che impedisce al prezzo di scendere al di sotto di un certo livello. Il supporto è un punto di prezzo in cui si prevede che un bene abbia una domanda significativa. Ciò indica che è improbabile che il prezzo scenda al di sotto di questo livello. Il supporto può essere valutato guardando un portafoglio ordini: il verificarsi di livelli di supporto è causato da una forte pressione all'acquisto in quella zona di prezzo, ma può anche essere correlato a grandi muri di acquisto che possono rendere più difficile un ulteriore calo del prezzo. I livelli di prezzo con una grande quantità di ordini di acquisto in sospeso sarebbero considerati livelli di supporto. In quanto tale, ci si aspetta che un livello di supporto agisca come un "pavimento" ed è solitamente causato da una grande offerta di acquirenti in una determinata regione di prezzo. Quindi possiamo considerare i livelli di supporto come punti in cui il prezzo può crollare solo con una forte pressione di vendita. In generale, trader e grafici tracciano linee di supporto basate sui minimi precedenti, il supporto può essere determinato dai movimenti storici dei prezzi. Questo approccio può tornare utile quando si cerca di prevedere potenziali punti di inversione del prezzo, che potrebbero indicare una buona opportunità di acquisto.

Il supporto può essere un prezzo costante, e sebbene siano per lo più rappresentati come linee orizzontali diritte, i livelli di supporto possono anche essere rappresentati da diagonali oppure può essere una linea di tendenza che aumenta o diminuisce nel tempo. Tuttavia, le diagonali sono generalmente chiamate linee di tendenza. Quando un livello di supporto viene interrotto, tende a diventare un livello di resistenza, che quindi presenterebbe un effetto opposto. Quindi, invece di fungere da supporto, la linea agirebbe ora come resistenza, agendo come un tetto che probabilmente impedirà al prezzo di salire ulteriormente. In genere, si verificano buone opportunità di trading quando i livelli di resistenza o di supporto vengono infranti. Quando si disegnano linee o zone di supporto, si consiglia di considerare almeno due minimi precedenti (idealmente tre o più). Più punti si usano per sostenere una analisi, più sarà affidabile. Lo stesso vale quando si disegnano le linee di resistenza e di tendenza. Tuttavia, come la maggior parte degli strumenti e degli indicatori di analisi tecnica, fare affidamento solo sulle linee di supporto e resistenza può essere molto rischioso. Per ridurre i rischi, è consigliato combinare l'uso di tali strumenti con un'analisi fondamentale adeguata, nonché altri indicatori tecnici. Il supporto è una variabile decisionale comune per i trader attivi.

Swap

Livello: avanzato

Argomento: finanza

Lo swap è lo scambio che effettua da una coin a un'altra attraverso l'uso di un DEX, ad esempio scambiare (o swappare) ETH in USDC.

sweep

spazzolamento

Livello: intermedio

Argomento: tecnologia

Lo sweep (a volte tradotto in italiano con *spazzolamento*) di una chiave privata nel contesto Bitcoin è un'operazione che trasferisce tutti i Bitcoin associati a quella chiave privata verso un nuovo indirizzo Bitcoin nel tuo portafoglio software.
Questo processo avviene tramite una transazione Bitcoin, quindi è necessaria una connessione internet per inviare la transazione e completare lo sweep.

In pratica, lo sweep è simile all'importazione di una chiave privata, ma con un passo aggiuntivo: dopo lo sweep, il vecchio portafoglio di carta o l'indirizzo originale della chiave privata sarà completamente svuotato dei fondi, e tutti i Bitcoin saranno trasferiti al nuovo indirizzo nel portafoglio software[1][1]. Questo è particolarmente utile e più sicuro se la chiave privata è stata precedentemente esposta o condivisa, perché impedisce ad altri di avere accesso ai Bitcoin una volta completato lo sweep.

Lo sweep comporta l'invio di una transazione (a te stesso), e quindi come tale ha un costo in termini di fee.

SWIFT

Acronimo di: Society for Worldwide Interbank Financial Telecommunication

Società per la Telecomunicazione Finanziaria Interbancaria Mondiale

Livello: intermedio

Argomento: politica

Swift, che sta per Society for Worldwide Interbank Financial Telecommunication, è sia la società cooperativa fondata nel 1973 e con sede a Bruxelles, che il suo sistema di trasferimento degli ordini, scambi in valuta, vendite e acquisti principalmente tra le banche che aderiscono a questo circuito.

Su Swift non viaggia il denaro ma i messaggi con le istruzioni necessarie per trasferire i fondi, praticamente l'indirizzo a cui spedirlo. Tutto avviene attraverso un codice: una stringa di numeri e lettere, tra gli 8 e gli 11 caratteri, che consente di effettuare pagamenti sicuri tramite banche in Paesi diversi.

La SWIFT è supervisionata dalle banche centrali del G-10 (Belgio, Canada, Francia, Germania, Italia, Giappone, Paesi Bassi, Regno Unito, Stati Uniti, Svizzera e Svezia) e dalla Banca centrale europea, con la Banca nazionale del Belgio come supervisore principale.

Nel 2022 il circuito è stato utilizzato per imporre sanzioni alla Russia, escludendola dal circuito.

Sybil attack

Attacco di Sybil

Livello: avanzato

Argomento: tecnologia

Un Sybil attack (dal nome della prima persona a cui è stato diagnosticato un disturbo di personalità multipla) è uno in cui qualcuno può creare molti nodi che fingono di essere nodi onesti, ma in realtà sono dannosi, al fine di indurre un nodo onesto ad accettare dati non validi o non veritieri, o in altro modo costringerlo a comportarsi in modo fuorviante.

L'invenzione del Nakamoto Consensus (ovvero il fatto che Bitcoin si affidi alla Proof of Work come meccanismo di verifica) è stata letteralmente progettata per prevenire i Sybil attack. Satoshi voleva che qualsiasi partecipante fosse in grado di aggiungere un blocco, ma la scelta di un utente a caso sarebbe stata aperta a individui che fingevano di essere molti utenti. Ma il lavoro non può essere falsificato, e questo è uno dei motivi per cui Bitcoin utilizza Proof of Work.

Gli attacchi Sybil non possono indurre un nodo Bitcoin ad accettare una copia falsa della blockchain. Per il nodo è sufficiente una sola connessione a un nodo onesto per essere resiliente a questo attacco a causa del consenso che Bitcoin sia basato sulla catena più lunga, o più precisamente la catena con la prova del maggior uso di potenza di elaborazione, quale copia più affidabile. Non è sufficiente che l'attaccante prenda il controllo del 99% della rete.

C'è un alto costo per il Sybil attack in Bitcoin per quanto riguarda il mining: la produzione di blocchi validi richiede l'utilizzo di energia del mondo reale. Un miner malintenzionato dovrebbe consumare una notevole energia nel mondo reale per produrre blocchi (comunque validi) per far consumare la catena delle transazioni. Un miner che produce blocchi non validi consuma semplicemente energia e perde denaro.

TA

Acronimo di: Technical Analysis

Analisi Tecnica

Livello: avanzato

Argomento: finanza

L'analisi tecnica è uno strumento utilizzato per studiare i mercati finanziari attraverso l'analisi di dati di mercato passati e presenti, con l'obiettivo di individuare modelli e tendenze che possano permettere di prevedere i movimenti futuri dei prezzi.

In generale, l'analisi tecnica si basa sull'idea che i movimenti passati del prezzo di un asset possano fornire informazioni utili per prevedere i suoi movimenti futuri. Si avvale di una varietà di strumenti e indicatori, tra cui:

Grafici: i grafici dei prezzi mostrano l'andamento del prezzo di un asset nel tempo. Vengono utilizzati per identificare modelli di prezzo e tendenze. Indicatori: gli indicatori sono strumenti matematici che vengono applicati ai dati di prezzo per generare segnali di trading. Gli indicatori possono essere utilizzati per identificare il momento in cui comprare o vendere un asset, misurare la volatilità del mercato e altro ancora.

Nel contesto specifico del bitcoin, l'analisi tecnica viene spesso impiegata dagli investitori e dai trader per cercare di anticipare i movimenti di prezzo della criptovaluta. Dato che il mercato del bitcoin è noto per la sua volatilità e per la mancanza di dati fondamentali tradizionali (come quelli di un'azienda), l'analisi tecnica diventa particolarmente importante per cercare di comprendere le dinamiche di mercato e prendere decisioni di trading informate.

Gli analisti tecnici di bitcoin esaminano i grafici dei prezzi del bitcoin e applicano gli stessi principi generali dell'analisi tecnica ad altre attività. Possono cercare modelli di tendenze, supporti e resistenze chiave, livelli di sovracomprato o ipervenduto, e altri indicatori per cercare di capire in che direzione potrebbe muoversi il prezzo del bitcoin nel breve e nel lungo termine.

Taint

Livello: avanzato

Argomento: legale

Con il termine taint (contaminate), poiché tramite blockchain i un certo modo è possibile tracciare il percorso delle transazioni, si vuole indicare la possibilità che alcune monete possano creare dei problemi ad esempio perché hanno una storia di utilizzo in attività criminali. La contaminazione è nella migliore delle ipotesi una misura probabilistica di quanto sia connessa una moneta con l'attività criminale passata. Taint è un termine soggettivo e viene applicato da diverse società di analisi della catena in base alle euristiche e alle ipotesi che impiegano.

Taker

Livello: intermedio

Argomento: finanza

Il "taker" è qualcuno che decide di effettuare un ordine che viene immediatamente abbinato a un ordine esistente nell'order book.

Un ordine taker si verifica quando un trader inserisce un ordine che viene eseguito immediatamente abbinandolo a un ordine maker esistente sull'order book di una borsa o di un exchange.
Ciò avverrà sempre con un ordine di mercato e può verificarsi anche con un ordine limite che ha un prezzo limite che può essere raggiunto immediatamente.
Gli ordini taker rimuovono la liquidità dal portafoglio ordini di una borsa.
È normale che gli scambi addebitino commissioni più elevate agli ordini taker a causa della rimozione di liquidità.

Tangle

Livello: avanzato

Argomento: tecnologia

"The Tangle" è un'alternativa blockchain sviluppata da IOTA, che utilizza grafici aciclici diretti che si costruiscono in una sola direzione e in un modo che non si ripete mai, ed è resistente ai calcoli quantistici.

TAP

Acronimo di: Taproot Assets Protocol

Livello: avanzato

Argomento: tecnologia

Taproot Assets, o TAP Taproot Assets Protocol, precedentemente chiamato Taro, è un meta-protocollo Bitcoin basato su Taproot, proposto ad aprile 2022 da Lightning Labs rilasciato nella sua prima versione alpha a settembre 2022, e a ottobre 2023 la prima release sulla mainnet, con l'alpha del daemon di Taproot Assets per mainnet, che fornisce un'esperienza di sviluppo completa per l'emissione, la gestione e l'esplorazione di stablecoin o altri asset, release introduce anche la compatibilità futura, il che significa che il protocollo non avrà più modifiche radicali che potrebbero influenzare gli asset emessi sulla mainnet. Questa release della mainnet del protocollo supporta le funzionalità on-chain, con il supporto Lightning Network in arrivo a breve.

Il significato di asset in questo contesto è analogo a quello di token, termine però poco gradito alla comunità Bitcoin.

Questi asset possono essere fungibili come le stablecoin, e non fungibili o NFT.

Non è il primo progetto per la creazione di asset o token su Bitcoin, ad esempio prima di TAP è stato presentato RGB, ma è il primo a fare uso dell'aggiornamento Taproot di Bitcoin per rendere l'implementazione più elegante e scalabile.

TAP combina sei componenti della tecnologia Bitcoin:

- La **rete Bitcoin** per la sicurezza e la stabilità, in quanto tutti gli asset TAP sono ancorati alla blockchain Bitcoin. Ciò significa che questi asset fanno parte di un pezzo di dati con hash che è collegato a una transazione nella blockchain. Grazie alla stabilità e all'elevato livello di sicurezza della rete Bitcoin, l'utente può essere certo che i suoi asset TAP siano sempre sicuri e trasferibili.
- **Lightning Network** per velocità, scala e commissioni ridotte. Analogamente al trasferimento di satoshis, è più economico, più veloce e più scalabile trasferire le attività di TAP su Lightning. Nel maggio 2024 Olaoluwa Osuntokun, co-founder e CTO di Lightning Labs, ha eseguito il primo multi-hop asset payment nella mainnet Bitcoin utilizzando Taproot Asset channels
- **Taproot**, l'aggiornamento apportato a Bitcoin nel 2021, viene utilizzato per incorporare i metadati degli asset in un input di transazione esistente.
- Le **firme Schnorr** sono utilizzate per semplificare e migliorare la scalabilità.
- i **Sparse Merkle Tree** consentono di recuperare e aggiornare i dati delle transazioni in modo rapido, efficiente e privato.
- I **Merkle Sum Tree** sono utilizzati per dimostrare che non sono stati creati nuovi asset e che non c'è inflazione, senza dover rivelare tutte le informazioni a nessun osservatore.

Nel suo nucleo, TAP sfrutta la sicurezza e la stabilità della rete bitcoin e la velocità, la scalabilità e le basse commissioni di Lightning.

Taproot Assets non utilizza Bitcoin come layer per la disponibilità completa dei dati (proprio come Lightning Network). Gli utenti di default archiviano i propri dati o si può aggiungere un ulteriore archiviazione dei dati off-chain con presupposto di attendibilità chiamato Asset Universe.

Gli asset TAP possono essere trasferiti sulla rete Bitcoin attraverso una transazione on-chain e anche istantaneamente, a basso costo e in modo più privato sulla rete Lightning quando vengono depositati in un canale.

TAP utilizza una struttura dati ad albero chiamata Sparse Merkle tree di Taproot che consente agli sviluppatori di incorporare metadati di asset arbitrari all'interno di un output UTXO esistente che consente il recupero e aggiornamento rapido, efficiente e privato dei dati witness/transazioni e un MS-SMT merkle-sum Sparse Merkle tree per la dimostrazione della valida conservazione/non inflazionistica.

Utilizza le firme Schnorr per migliorare la semplicità e la scalabilità e, cosa

importante, funziona con le transazioni multi-hop su Lightning.

Nel corso della storia di Bitcoin, sono state avanzate diverse proposte per portare gli asset sulla blockchain di Bitcoin. TAP porta avanti queste idee concentrandosi su ciò che Taproot consente di fare in questo campo. Con un design incentrato su Taproot, TAP può fornire asset su Bitcoin e Lightning in modo più privato e scalabile. Gli asset emessi su TAP possono essere depositati nei canali della rete Lightning, dove i nodi possono offrire conversioni atomiche da Bitcoin ad asset TAP. Ciò consente agli asset TAP di essere interoperabili e trasferibili con Lightning Network, beneficiando della sua portata e rafforzando i suoi effetti di rete.

I partecipanti al trasferimento di TAP sostengono i costi di verifica e archiviazione memorizzando i dati del witness TAP off-chain negli Asset Universe, simili a un repository git.

Per controllare la validità di un asset TAP, si verifica il suo percorso dall'uscita della genesi. Questo si ottiene ricevendo un file di verifica dei dati delle transazioni attraverso il gossip layer di TAP. I client possono fare un controllo incrociato con la loro copia della blockchain e modificare con le proprie prove il passaggio dell'asset.

Gli asset di TAP sono registrati sulla blockchain di Bitcoin sotto forma di metadati con hash allegati a una transazione. La memorizzazione di tutti i metadati direttamente sulla blockchain occuperebbe più spazio e sarebbe quindi più costosa. Questo costo viene evitato utilizzando un hash.

Per inviare asset TAP a un'altra persona, questa dovrà prima fornirvi il suo indirizzo TAP. Questo indirizzo contiene le informazioni sull'asset e le chiavi pubbliche necessarie per il suo mantenimento. Il formato dell'indirizzo è stato progettato per evitare che gli asset TAP vadano persi o siano irrecuperabili.

Poiché non ci sono limiti alla quantità di dati che possono essere rappresentati da un hash, una transazione sulla blockchain può rappresentare milioni di transazioni. Questo vale anche per i trasferimenti di asset TAP.

NFT su TAP Gli asset non fungibili, o NFT, sono emessi in un lotto unico e limitato in una transazione on-chain. Questi asset non possono essere divisi o uniti, ma possono solo cambiare proprietà, il che avviene off-chain trasferendo l'identificativo unico dell'asset e il suo file di verifica dei dati storici delle transazioni che ne provano l'autenticità. Queste informazioni sono memorizzate negli Asset Universe che svolgono un ruolo simile a quello di un block explorer e possono essere gestiti da chiunque sia interessato agli asset.

Il nuovo proprietario di un asset TAP può esaminare i dati in un TAP Asset Universe e usarli per ricostruire i metadati nella blockchain e verificare la proprietà. Può anche modificare i metadati con le proprie prove prima di trasmettere l'asset.

Stablecoin su TAP Un asset fungibile su TAP, come una stablecoin, può essere diviso e unito. Ciò significa che se un utente possiede un asset, può cambiare proprietà all'interno di un gruppo esistente di utenti che hanno tutti asset all'interno dello stesso Merkle tree, oppure gli asset possono essere trasferiti a un utente in un Merkle tree diverso. Una versione aggiornata del Merkle tree mostrerebbe semplicemente che l'offerta totale dell'asset non è cambiata, ma i saldi dei diversi proprietari sono stati aggiornati.

Trasferire un asset TAP Gli asset TAP hanno regole specifiche su come interagire con esse e convalidarle. Queste regole sono memorizzate nello script dell'asset, un insieme di regole create da uno sviluppatore che definiscono come questo specifico asset può essere trasferito. Questo asset script diventa parte del Merkle-Sum Sparse Merkle tree.

La conoscenza di come gestire gli asset TAP deve essere trasferita al nuovo proprietario, in modo che quest'ultimo sappia come trasferire l'asset dopo averlo ricevuto e possa dimostrare al proprietario successivo di avere questa conoscenza. Per rendere questo possibile, TAP utilizzerà un formato di indirizzo basato su bech32 che includerà l'hash dello script dell'asset. Il proprietario può quindi dimostrare di essere a conoscenza di come spendere questo asset TAP, fornendo l'asset script al proprietario successivo, che può eseguire l'hash per verificare che corrisponda all'hash dell'asset script allegato.

TAP su Lightning Gli asset emessi su TAP possono essere depositati nei canali della rete Lightning e transati istantaneamente.

Questo principio consente agli utenti della Lightning Network di detenere nel proprio wallet un saldo diverso da BTC: ad esempio, una stablecoin. Possono ricevere pagamenti denominati in stablecoin e utilizzare il loro saldo in stablecoin per pagare beni e servizi attraverso Lightning Network. Bitcoin rimane la spina dorsale di Lightning Network e i pagamenti attraverso gli asset TAP possono essere instradati sull'attuale Lightning Network, senza la necessità di effettuare un upgrade o un opt-in. Con Bitcoin che fornisce la liquidità per questi pagamenti denominati in altri asset, l'instradamento degli asset TAP può fornire maggiori commissioni di instradamento pagate in satoshi per gli operatori dei nodi di instradamento.

Tapering

Livello: avanzato

Argomento: politica

In economia, il tapering è la riduzione graduale della quantità di denaro che viene iniettata nel sistema economico attraverso acquisti di attività da parte di una banca centrale. Il tapering è l'inversione teorica delle politiche di QE, Quantitative Easing, attuate da una banca centrale. Le attività di tapering

sono principalmente rivolti ai tassi di interesse e al controllo delle percezioni degli investitori sulla direzione futura dei tassi di interesse. Le attività di tapering possono includere la modifica del tasso di sconto o dei requisiti di riserva. Il tapering può anche comportare il rallentamento degli acquisti di asset da una banca centrale. Il tapering viene effettuato dopo che le politiche di QE hanno ottenuto l'effetto desiderato di stimolare e stabilizzare l'economia. Il tapering può essere effettuato solo dopo che è già stato attivato un qualche tipo di programma di stimolo economico.

Taproot

Livello: intermedio

Argomento: tecnologia

Taproot è il nome dato ad un aggiornamento del protocollo Bitcoin con adottato in modalità soft fork nel novembre 2021. È il più grande aggiornamento della rete Bitcoin, almeno da quello che ha introdotto SegWit nel 2017. Dovrebbe migliorare la scalabilità, la privacy e la sicurezza delle rete Bitcoin.

La differenza principale delle transazioni Taproot rispetto alle transazioni Bitcoin convenzionali è che gli script che controllano le monete sono contenuti all'interno di una struttura ad albero chiamata ramo tapScript che è impegnata privatamente nella transazione. Questi script non hanno bisogno di essere rivelati se il KeySpend Path viene utilizzato per spostare le monete. Mentre una transazione convenzionale richiede che l'intero script sia rivelato, una transazione Taproot può essere spesa con una chiave che evita di rivelare gli script e se il KeySpend Path non è fattibile, solo la parte eseguita dello script viene rivelata sulla blockchain. Tutti gli altri percorsi degli script possono rimanere privati, o essere rivelati selettivamente off-chain. Questo rende possibile creare script più complicati senza il costo aggiunto di presentare dati extra alla blockchain nel KeySpend Path, e una verifica efficiente dei dati pruned di uno script.

BIP 340, BIP 341 e BIP 342 sono parte integrante dell'aggiornamento Taproot

Tapscript

Livello: avanzato

Argomento: tecnologia

Tapscript è il linguaggio di scripting utilizzato per abilitare su bitcoin una varietà di nuovi tipi di transazione come parte dell'aggiornamento Taproot. Tapscript è il linguaggio di scripting usato per gli script-path di taproot.

Condivide la maggior parte delle operazioni con gli script Bitcoin legacy e SegWit, ma presenta alcune differenze:

OP_CHECKMULTISIG e OP_CHECKMULTISIGVERIFY sono sostituiti dall'opcode OP_CHECKSIGADD. OP_CHECKSIGADD, sfrutta il fatto che le firme Schnorr, un altro aspetto dell'aggiornamento Taproot, possono essere aggregate.

Molti opcode precedentemente disabilitati sono stati ridefiniti come opcode OP_SUCCESS che rendono incondizionatamente valido l'intero script per semplificare gli aggiornamenti soft fork.

Gli hash delle firme sono calcolati in modo diverso rispetto allo script legacy o al segwit BIP143 v0.

taptweak

Livello: avanzato

Argomento: tecnologia

Una transazione che vincola dei dati arbitrari viene definita commitment.

Una volta che la transazione è stata inserita in un blocco on-chain, abbiamo un commitment su questi dati e non possiamo più cambiarli o modificarli.

Per effettuare il commitment ai dati, modifichiamo la chiave pubblica della nostra chiave di spesa Taproot utilizzando un trucco noto come **Taptweak**. Questo ci permette di rivelare selettivamente i dati senza rivelare la chiave privata, o di spendere l'output senza rivelare il commitment.

Questa tecnica viene utilizzata nelle transazioni Taproot per impegnarsi (commit) nell'albero degli script Taproot e può essere utilizzata per impegnarsi in qualsiasi dato arbitrario.

```
Q= P+H(P|c)G
```

Dove:

- `Q` è la chiave pubblica finale di Taproot
- `P` è la chiave pubblica interna
- `H(P|c)` è l'hash della chiave pubblica interna e del commitment.

Per firmare una transazione con la nostra chiave privata, la chiave privata deve essere modificata con lo stesso hash della chiave pubblica e del commitment, `H(P|c)`.

Target hash

Livello: avanzato

Argomento: tecnologia

Il Target hash è un numero a 256 bit condiviso da tutti i client Bitcoin.

Questo numero viene utilizzato dall'algoritmo della Proof of work per fare in modo che i miner debbano fare dei calcoli di una certa complessità, o difficulty.

I miner devono provare il nonce fino a quando non riescono ad ottenere il target hash.

Ogni hash è fondamentalmente un numero compreso tra 0 e il valore massimo di un numero a 256 bit (che è enorme). Se l'hash calcolato dal miner è al di sotto del target, allora ha generato un blocco valido che può essere aggiunto alla blockchain, in caso contrario incrementa il nonce per generare un nuovo hash, e continua così fino a quando non ottiene un hash valido.

Il target è codificato come parte del block header di ciascun blocco ed è chiamato 'bits' di un blocco. Ciò consente ai nodi di verificare direttamente se la prova di lavoro fornita per un blocco è inferiore all'obiettivo.

L'hash SHA-256 dell'header di un blocco deve essere inferiore o uguale al target hash corrente affinché il blocco venga accettato dalla rete. Più basso è il target, più difficile è generare un blocco.

Il Target hash si modifica con le stesse regole della difficulty (sono infatti sono due elementi della stessa equazione): ogni 2016 blocchi minati (che dovrebbero richiedere due settimane se si mantiene la media di un blocco minato ogni 10 minuti), ogni client Bitcoin confronta il tempo effettivo impiegato per generare questi blocchi con l'obiettivo di due settimane e modifica l'obiettivo della differenza percentuale. Questo rende il problema del proof-of-work più o meno difficile. Un singolo retarget non cambia mai il target oltre un fattore 4 per evitare grandi cambiamenti di difficoltà.

taro

Acronimo di: Taproot Asset Representation Overlay

Livello: avanzato

Argomento: tecnologia

Il protocollo Taro, acronimo di Taproot Asset Representation Overlay, è stato annunciato da Lightning Labs nell'aprile 2022 come un sistema per l'emissione di asset tokenizzati sulla blockchain di Bitcoin utilizzando l'aggiornamento Taproot.

Successivamente, nel ottobre 2023, Lightning Labs ha rinominato il protocollo Taro in Taproot Assets Protocol, in seguito a una disputa legale sul nome "Taro" con Tari Labs.

È un protocollo di tipo CSV Client-side validation, utilizza la struttura di commitment di taproot per consentire alle transazioni il commit di dati aggiuntivi. La costruzione di Taproot deriva anch'essa dal pay-to-contract. Come suggerisce il nome, lo sviluppo iniziale del protocollo è specificamente focalizzato sul trasferimento di asset (ossia, token digitali che rappresentano asset).

Alcuni sostengono che TARO si sia ispirato a RGB.

Testnet

Livello: intermedio

Argomento: tecnologia

La testnet è una blockchain alternativa utilizzata dagli sviluppatori per testare le varie funzionalità della piattaforma nella quale le monete non hanno valore reale.
Si contrappone alla blockchain in produzione e operativa, definita mainnet.

La testnet è una rete P2P completa, dotata di tutte le funzionalità, inclusi wallet, bitcoin di test (monete testnet), mining e tutte le altre caratteristiche della mainnet.

La differenza più importante è che le monete testnet dovrebbero essere prive di valore. Ogni sviluppo software destinato all'uso sulla rete principale di Bitcoin può essere testato preventivamente su testnet con monete di prova. Ciò protegge sia gli sviluppatori da perdite monetarie dovute a bug, sia la rete da comportamenti indesiderati causati da bug.

La testnet utilizza le stesse strutture dati di Bitcoin e lo stesso meccanismo di sicurezza PoW, proof-of-work.

Con la testnet, anche i miner possono testare le proprie attrezzature e infrastrutture per generare blocchi in un ambiente di test.

Le principali differenze tra testnet e mainnet sono le seguenti:

- la difficoltà su testnet è equivalente a una difficoltà di metà su mainnet (1,0 su testnet corrisponde a 0,5 su mainnet). Questo significa che qualsiasi difficoltà su testnet è il doppio di quella su mainnet.;
- la *minimum difficulty rule*, o regola della difficoltà mininma, stabilisce che se non viene trovato alcun blocco per 20 minuti, la difficoltà si reimposta automaticamente al valore minimo per un blocco singolo, prima di ritornare al valore precedente (con una eccezione nel caso del blocco retarget, di seguito spiegato);
- è disabilitato il controllo di validità delle transazioni standard (*IsStandard()*), in modo che sia possibile sperimentare transazioni non standard
- gli indirizzi testnet hanno un formato diverso (un valore diverso del campo ADDRESSVERSION) per garantire che non possano funzionare sulla mainnet

Il meccanismo PoW di Bitcoin dipende da incentivi economici che non esistono nella testnet, dove le transazioni contengono commissioni che non dovrebbero avere un valore economico.

Sulla mainnet, i miner sono incentivati a includere le transazioni degli utenti nei loro blocchi perché tali transazioni pagano commissioni.

Su testnet, le transazioni contengono ancora qualcosa chiamato commissioni, ma tali commissioni non hanno un corrispondente valore economico. Ciò significa che l'unico incentivo per un miner testnet ad includere transazioni è perché o vuole testare le funzioni del mining, o vuole aiutare gli utenti e gli sviluppatori a testare il proprio software.
Poiché il mining PoW è progettato per essere senza autorizzazione, chiunque può eseguire il mining, indipendentemente dal fatto che la sua intenzione sia buona o meno. Ciò consente ad esempio che i miner possono creare molti blocchi di seguito su testnet senza includere alcuna transazione dell'utente.
Quando si verificano questi attacchi, la testnet diventa inutilizzabile per utenti e sviluppatori.

La difficoltà di estrazione dovrebbe essere abbastanza bassa da permettere a chiunque di fare mining testnet in modo relativamente semplice.

La testnet ha la caratteristica che garantisce che si possa essere in grado di estrarre blocchi se i suoi più grandi miner la abbandonano improvvisamente: la difficoltà minima di 1,0 su testnet è uguale a una difficoltà di 0,5 su mainnet. Ciò significa che l'equivalente mainnet di qualsiasi difficoltà del testnet è la metà della difficoltà di testnet.

Nonostante le richieste di utilizzare equipaggiamento low-end da parte degli sviluppatori, i miner testano su testnet le loro attrezzature da mining avanzate (GPU e ASIC).

Ciò può far aumentare la difficoltà rendendo impossibile minare con una CPU, e di conseguenza rende altrettanto difficile ottenere monete di prova e le persone hanno iniziato a darne un valore, rendendole non realmente inutili e prive di valore.

Testnet3 Di tanto in tanto, la testnet dovrebbe essere scartata e riavviata da un nuovo genesis block, ripristinando la difficoltà e scartando le transazioni.

L'attuale testnet è chiamata testnet3, la terza iterazione di testnet, riavviata a febbraio 2011.

La prima versione di testnet è stata avviate il 19 ottobre 2010, per consentire agli sviluppatori di testare le modifiche al software senza modificare la main net.
La versione precedente rispetto all'attuale ha iniziato ad avere una elevata difficoltà, e a causa di questo le monete testnet sono diventate scarse e molti utenti ne hanno approfittato per venderle.
L'idea del riavvio dovrebbe essere proprio quella di evitare questo incentivo a creare un mercato per le monete testnet.

La vulnerabilità Timewarp della testnet Il meccanismo di PoW della testnet, che ha dei parametri leggermente diversi da quello della mainnet Bitcoin, soffre di una vulnerabilità chiamata Timewarp.

Così come succede con la mainnet bitcoin, anche testnet ricalcola la difficulty di mining ogni 2016 blocchi.

La difficoltà viene regolata regolarmente in modo da mirare a un intervallo di blocco medio di 10 minuti, ma non tutti gli intervalli di blocco sono esattamente di 10 minuti.
La distribuzione dei blocchi nel tempo segue un processo statistico noto come processo di Poisson, secondo la quale eventi casuali si verificano con la stessa probabilità in ogni intervallo di tempo.

Poiché per il mining della testnet non ci sono gli stessi incentivi economici che esistono sulla mainnet, l'hashrate della testnet può variare in modo sostanziale, poiché uno dei partecipanti al mining testnet potrebbe avere una grande potenza di calcolo rispetto agli altri partecipanti, portare la difficulty a valori molto alti e poi smettere di minare: questo impedisce agli altri miner di trovare un blocco in tempi relativamente brevi.

A causa dell'imprevedibilità della potenza di hashing e dei tempi del blocco, esiste una regola speciale nella testnet che consente di minare un blocco contro la difficoltà minima di 1 (e quindi praticamente istantaneamente su una GPU o ASIC) se non c'è stato un blocco per 20 minuti.
Questa funzionalità garantisce che gli utenti non debbano mai attendere più di 20 minuti per un blocco, anche se l'unico miner rimasto sulla rete ha un hardware poco potente.
Se non viene trovato alcun blocco entro 20 minuti, la difficoltà si reimposta automaticamente al minimo per un singolo blocco, dopodiché ritorna al valore precedente.
Questa regola viene invocata abbastanza regolarmente su testnet.
Secondo alcuni studi quasi 200.000 blocchi (circa il 12% di tutti i blocchi) su testnet sono stati estratti con una difficoltà pari a 1 dopo che è trascorsa la finestra di 20 minuti dal blocco precedente.

Se questa diminuzione improvvisa della difficoltà avviene nel blocco del retarget, si genera un problema di tipo retarget overflow, chiamato Timewarp.
Questo problema avviene diverse volte all'anno, in modo naturale o provocato volutamente, che consente di effettuare un griefing attack e tramite questo fare un block storm ovvero inondare la testnet di un numero insolitamente elevato di blocchi che provocano con un tasso di orfani molto elevato.

Perché il ripristino della difficoltà causa tali conflitti con i servizi in esecuzione su testnet?
Mentre nella main net di solito in una giornata vengono minati circa 144 blocchi, se sulla testnet si verifica un ripristino della difficoltà al minimo, anche un ASIC economico può estrarre più blocchi al secondo.
Se si hanno diversi miner testnet che emettono blocchi sulla rete, ci saranno parecchi conflitti.

Quando un nodo Bitcoin riceve un nuovo insieme di blocchi in conflitto che hanno più prove di lavoro di quella che considera la migliore catena attuale,

deve eseguire una riorganizzazione della blockchain. Ciò comporta il rollback sequenziale dell'attuale catena di blocchi e transazioni e quindi l'applicazione della nuova catena: è un processo molto intenso che avviene molto raramente sulla main net e quasi mai con più di un blocco alla volta.
Molti nodi o servizi scritti in modo approssimativo eseguiranno semplicemente questa operazione in memoria per avere un miglioramento delle prestazioni, ma quando ricevono una riorganizzazione che ha centinaia o migliaia di blocchi la macchina potrebbe esaurire la memoria e causare il crash del nodo o del servizio, congelandolo così all'ultimo blocco elaborato con successo.
È anche possibile che il servizio non abbia un blocco attorno a questa operazione e se è nel mezzo di un'esecuzione di riorganizzazione mentre si verifica un'altra riorganizzazione, il servizio bloccherà/bloccherà/corromperà i dati.

Testnet4/BIP94 A partire da Bitcoin core 28.0, rilasciato a ottobre 2024, è stato aggiunto il supporto per Testnet4 come specificato in BIP94. Può essere selezionata tramite l'opzione
`-testnet4`

Sebbene l'intenzione sia quella di eliminare gradualmente il supporto per Testnet3 in una versione futura, è ancora disponibile tramite le opzioni note in questa versione.

Testnet4 include la correzione della regolazione della difficoltà PoW e corregge i bug della regolazione della difficoltà e del time warp.

Altri tipi di test net Per gli sviluppatori, alcune caratteristiche della testnet come l'imprevedibilità della creazione dei blocchi e dell'inclusione delle transazioni può essere un problema, con i miner che si uniscono e lasciano la rete in modo imprevedibile.
Inoltre, poiché i miner spesso testano le proprie impostazioni su questa rete, non sempre includono le transazioni che gli sviluppatori si aspettano.

Per questi motivi sono state create delle diverse forme di testnet:

- Signet
- Segnet
- modalità regtest

TFR

Acronimo di: Transfer of Funds Regulation

Regolamento sui Trasferimenti di Fondi

Livello: intermedio

Argomento: legale

Il TFR, Transfer of Funds Regulation o Regolamento sui Trasferimenti di Fondi, è una legge del parlamento Europeo che, adducendo la solita motivazione di contrastare il riciclaggio di denaro (AML) e il finanziamento del terrorismo (CTF), impone a gli operatori di servizi sulle cripto, CASP o VASP Europei un vasto regime di sorveglianza finanziaria compromettendo anche la privacy dei wallet non-custodial (definiti anche self-hosted).

Il TFR richiede ai CASP che tutte le transazioni di criptovalute, senza una soglia minima di transazione, dovranno raccogliere, verificare e presentare determinate informazioni sull'ordinante (ossia una persona che detiene un conto o un indirizzo di cripto-asset) e sul beneficiario (ossia una persona che è il destinatario previsto del trasferimento di cripto-asset) dei trasferimenti di cripto-asset, la cosiddetta Travel Rule.

Quando effettuano transazioni con wallet non-custodial, i CASP europei devono raccogliere le informazioni richieste sull'ordinante e sul beneficiario e in caso di trasferimento a un wallet non-custodial per importi superiori ai 1000 euro il VASP ordinante è tenuto a verificare se tale wallet è di proprietà o controllato dal cliente ordinante, e quando riceve un trasferimento da un wallet non-custodial il VASP beneficiario deve verificare che il cliente beneficiario possieda o controlli il wallet di origine.
Questa verifica avviene chiedendo all'utente di firmare un messaggio con la stessa chiave privata del wallet di destinazione, operazione che potrebbe essere effettuata automaticamente dal contestato protocollo AOPP Address Ownership Proof Protocol, protocollo che era stato inizialmente implementato e poi rimosso da diversi sviluppatori di wallet.

Sono esenti queste limitazioni per i trasferimenti tra wallet non-custodial, anche perché praticamente impossibili da controllare, ma quando si ritirano i bitcoin da un exchange o si fanno transazioni con altri fornitori di servizi cripto viene creata una traccia.

Il 20 aprile 2023, il Parlamento europeo ha votato a favore della legge TFR con 529 voti a favore, 29 contrari e 14 astensioni.
La legge diventerà operativa contemporaneamente al MiCA, che è stato votato lo stesso giorno, e entrerà in vigore a gennaio 2025 per tutti i VASP, prestatori di servizi di virtual asset, 18 mesi dopo l'entrata in vigore del regolamento.

Applicato per la prima volta ai sistemi di pagamento tradizionali nel 2015, il TFR è stato ampliato per coprire anche i trasferimenti di criptovalute. Si tratta dell'attuazione da parte dell'UE della Travel Rule del GAFI Gruppo d'azione finanziaria.
Tuttavia, il TFR si spinge oltre le raccomandazioni del GAFI.

Thiers' Law

legge di Thiers

Livello: avanzato

Argomento: politica

La legge di Thiers afferma che il denaro buono scaccia il denaro cattivo. È il complemento della legge di Gresham, che afferma il contrario, ovvero "la moneta cattiva scaccia quella buona".

La legge di Thiers è più applicabile quando una valuta perde così tanto valore da non essere più accettata come mezzo di pagamento dai commercianti. Nella maggior parte dei paesi, le leggi sul corso legale rendono illegale rifiutare la valuta locale come mezzo di pagamento, ma queste leggi vengono ignorate e diventano obsolete in condizioni come l'iperinflazione.

Sebbene la legge di Thiers e la legge di Gresham possano sembrare contraddittorie, non lo sono. Quando i cittadini sono liberi, tendono ad accettare e utilizzare un buon denaro, caratterizzato dalla sua capacità di immagazzinare valore e di fungere da mezzo di scambio. Quando viene loro negata la scelta, di solito dalle leggi sul corso legale, gli individui accumuleranno il denaro buono e spenderanno il denaro cattivo il più rapidamente possibile.

Tuttavia, le leggi sul corso legale possono proteggere il denaro cattivo solo fino ad un certo punto. Alla fine, la moneta cattiva diventerà praticamente inutile e i cittadini ignoreranno le leggi sul corso legale. Durante il periodo di iperinflazione dello Zimbabwe, molti cittadini hanno iniziato a utilizzare dollari statunitensi nonostante il loro divieto, e molte valute estere circolavano nella Repubblica di Weimar durante gli anni '20.

Ticker

Livello: base

Argomento: finanza

è il simbolo azionario o il nome abbreviato (generalmente in maiuscolo) utilizzato per identificare in modo univoco le azioni di un determinata azienda quotata in borsa e nelle criptovalute una moneta su una piattaforma di trading. Ad esempio BTC per i bitcoin, ETH per Ethereum

Timelock/Locktime

Livello: avanzato

Argomento: tecnologia

Timelock è una caratteristica che consente a Bitcoin di funzionare come denaro programmabile, impostando delle condizioni per cui una transazione viene elaborata solo in un certo momento o blocco della blockchain. Sono dei vincoli che impediscono che una transazione o la spesa di un output sia confermata prima di un tempo di maturazione o di un block height.

Un timelock permette di creare una transazione Bitcoin tale che il destinatario degli output non possa spenderli per un tempo specificato.

Il meccanismo di timelock è stato inizialmente inserito da Satoshi Nakamoto nel campo nLockTime.

Attualmente ci sono 4 tipi di timelock per Bitcoin:

- nLocktime
- nSequence
- CLTV CheckLockTimeVerify
- CSV CheckSquenceVerify

I timelock hanno 3 attributi:

- **Posizione**: a livello di transazione o a livello di script
- **Orientamento**: assoluto o relativo
- **Metrica**: block height (numero o altezza del blocco) o timestamp

Specchietto riassuntivo:

timelock	Posizione	Orientamento
nSequence	transazione	Relativo
nLocktime	transazione	Assoluto
CSV	script	Relativo
CLTV	script	Assoluto

Posizione

I timelock possono essere impostati nelle transazioni, e possono anche essere inclusi negli script.

Sono molto simili, ma svolgono funzioni completamente diverse. Se sono impostati a livello di transazione, i timelock non possono essere convalidati fino a che non si raggiunge un certo momento o una block height definita, sebbene le loro firme e script siano validi. I timelock a livello di script sono realizzati inserendo negli script delle condizioni che determinano quando uno script è valido, e le condizioni possono essere impostate su tutte le transazioni che spendono un output.

nLockTime e nSequence operano a livello di transazione, mentre CheckLockTimeVerify e CheckSquenceVerify operano a livello di script.

Orientamento

Gli orari dei timelock possono essere **assoluti** o **relativi**.

Quelli assoluti consentono di definire il lock secondo uno specifico orario, quindi si può scegliere il momento esatto in cui terminerà il blocco. Quelli relativi

consentono di definire un certo lasso di tempo che deve trascorrere a partire dalla conferma degli output precedenti. Entrambe le opzioni sono estremamente utili per definire gli intervalli di tempo necessari affinché una transazione venga elaborata dalla rete Bitcoin.

nLockTime e CheckLockTimeVerify sono timelock assoluti, mentre nSequence e CheckSquenceVerify sono timelock relativi

Metrica

In Bitcoin ci sono due modi per misurare il tempo: il **block height** (numero di blocco) e **timestamp**.

Quando si imposta un blocco temporale basato su un block height, i miner aspettano di raggiungere quel numero di blocco per poter validare e confermare l'operazione e includerla in un nuovo blocco.

Nel caso sia impostato il timestamp, i miner attendono fino ad arrivare al momento indicato dal timestamp. Il timestamp è espresso secondo il formato del timestamp Unix.

Formato del campo

Il campo Locktime è un campo a 4 byte (32 bit) che può essere espresso in due modi:

- Come un blocco numerico: Se il valore di Locktime è inferiore a 500 milioni, viene interpretato come il numero di blocco a partire dal quale la transazione può essere inserita nella blockchain. Ad esempio, se il valore di Locktime è 100, la transazione non potrà essere inserita nella blockchain prima del blocco numero 100.
- Come un timestamp: se il valore di Locktime è uguale o superiore a 500 milioni, viene interpretato come un timestamp UNIX (numero di secondi trascorsi dal 1 gennaio 1970). Ad esempio, se il valore di Locktime è 1498870928, la transazione non potrà essere inclusa nella blockchain prima delle 14:48:48 UTC del 1 luglio 2017.

Il campo Locktime è facoltativo e può essere omesso se non è necessario. Se Locktime non è presente nella transazione, la transazione può essere inserita immediatamente nella blockchain.

Se si imposta un nLocktime futuro, la transazione non potrà essere inserita nella blockchain fino a quel momento specifico, ma non deve neanche essere trasmessa agli altri nodi ma deve essere conservata: se si tenta di inviare una transazione con un nLocktime futuro alla rete Bitcoin prima del momento specificato, la transazione verrà respinta come non valida dal primo nodo che la riceve e non verrà trasmessa ad altri nodi.

Timestamp

Marca temporale

Livello: intermedio

Argomento: tecnologia

Un timestamp è una marca temporale che indica un preciso momento nel tempo. Può essere utilizzato per registrare quando è stato effettuato un determinato evento, ad esempio la data e l'ora di un blocco, di una transazione o di un messaggio.

Esistono diversi formati di timestamp, tra cui:

- **UNIX timestamp**: un numero intero che rappresenta il numero di secondi trascorsi dal 1° gennaio 1970, 00:00:00 UTC.
- **ISO 8601**: una stringa che segue il formato "YYYY-MM-DDTHH:mm:ss.sssZ", dove "T" separa la data dall'ora, ":" separa le unità di tempo e "Z" indica che l'ora è in UTC.
- **RFC 2822**: una stringa che segue il formato "Thu, 21 Dec 2000 16:01:07 +0200", utilizzato nei messaggi di posta elettronica.

Rispetto ai timestamp UNIX e ISO8601, il formato RFC2822 è meno preciso e più verboso ma più umanamente leggibile.

timewarp

Livello: avanzato

Argomento: tecnologia

Il bug Time-Warp, noto anche come "Timestamp Manipulation Attack", è una vulnerabilità che consente a un miner di effettuare un attacco attraverso la manipolazione dei timestamp sui blocchi che estrae.

Il bug è stato scoperto per la prima volta nel 2011 dall'utente BitcoinTalk "ArtForz".
ArtForz ha notato discrepanze nei timestamp dei blocchi estratti e ulteriori indagini hanno rivelato la vulnerabilità.

I vincoli dei timestamp dei blocchi possono essere raggirati facendo in modo che gli ultimi blocchi di una difficulty epoch vengano fissati in futuro con un timestamp impostato ad arte per regolare arbitrariamente la difficulty, seppur nei limiti minimo e massimo consentiti dall'algoritmo di regolazione della difficulty.

Il miner può scegliere quale data e orario inserire come timestamp nell'header del blocco, ma le regole di consenso impediscono di impostare un timestamp con valori troppo distanti dagli altri blocchi, richiedendo che qualsiasi timestamp debba essere maggiore del tempo mediano degli 11 blocchi precedenti, chiamato MTP o Median time-past.

Tuttavia, i miner che controllano la maggioranza dell'hashrate (o una sotto-maggioranza di miner che utilizzano un attacco che dà loro influenza sugli altri miner, come il selfish mining), potrebbero ottenere un controllo preciso sull'orario dell'header di ciascun blocco.

Modificando i timestamp in avanti, l'attaccante può far sembrare alla rete che la velocità di produzione dei blocchi sia molto più lenta di quanto lo sia effettivamente stata.
Il DAA, Difficulty Adjustment Algorithm, che regola la difficulty volta ogni 2016 blocchi per mantenere il tempo medio di creazione di un blocco a circa 10 minuti, potrebbe essere ridurre significativamente la difficulty.

I miner che iniziano un time warp attack non possono influenzare in modo significativo la difficulty per il primo blocco dell'epoca perché sia il primo che l'ultimo blocco di quell'epoca dovranno avere orari approssimativamente accurati. Per la successiva epoca, i miner possono far sembrare che il primo blocco sia stato estratto due settimane prima e che l'ultimo blocco sia stato estratto attualmente, fornendo una media di circa 20 minuti per blocco e inducendo la DAA a dimezzare la difficoltà.

I miner saranno quindi in grado di completare l'epoca successiva due volte più velocemente e tuttavia faranno sembrare che ci siano voluti circa 25 minuti per blocco, riducendo ulteriormente la difficulty. Possono così ripetere l'attacco indefinitamente finché non producono un blocco al secondo, il limite inferiore consentito dalla regola del Median time-past.

Una volta ridotta la difficulty, l'attaccante potrebbe iniziare a minare una serie di blocchi molto rapidamente, approfittando della difficulty artificiosamente bassa.

In questo modo il miner attaccante può creare un certo numero di blocchi che rilascia sulla rete.

Se l'attacco ha successo, la blockchain che l'attaccante sta diffondendo verrà considerata la versione corretta della blockchain, essendo più lunga e quindi considerata quella "giusta" secondo le regole di consenso di Bitcoin.

È fondamentale sottolineare che, considerati i valori di hashrate raggiunti dal mining di Bitcoin, l'attuazione di un attacco timewarp sulla rete mainnet è quasi impossibile e richiederebbe il controllo di una parte significativa dell'hashrate complessivo per un lungo periodo di tempo.
Al contrario, su testnet, l'esecuzione di tale attacco risulta decisamente più semplice, al punto possono essere creati dei block storm come dimostrato da diversi casi documentati e sono così stati effettuati griefing attack.

Attraverso questi block storm l'inflazione programmata delle monete viene accelerata e l'offerta massima o Max Supply di 21 milioni di Bitcoin in circolazione verrebbe raggiunto più velocemente del suo programma naturale di emissione, come infatti sta avvenendo nella testnet che nonostante sia stata avviata nel

2011 ha oltre 3 volte tanto i blocchi della mainnet, con una media di un blocco ogni 2 minuti invece di 10.

To the moon!

Livello: base

Argomento: politica

Letteralmente traducibile in "Verso la luna!", è un gergo utilizzato dagli utenti entusiasti quando il prezzo di una moneta ha un forte rialzo, oltre le aspettative. Viene anche utilizzato dai trolls per creare hype o come "augurio" per una moneta appena lanciata, come un "buona fortuna" o un "in bocca al lupo".

Token

Livello: base

Argomento: tecnologia

A volte usato come sinonimo di coin, token è più in generale usato in modo diverso da coin.

Si tratta di unità di valore digitali non minabili che esistono come voci di registro nelle blockchain. I token sono disponibili in molte forme diverse: possono essere utilizzati come valute per ecosistemi specifici ed essere fungibili o non fungibili (vedi NTF). Alcuni token potrebbero essere riscattabili per commodity off-chain. I token sono generalmente emessi da aziende che utilizzano blockchain di terze parti esistenti come la blockchain di Ethereum, come esemplificato dai numerosi token ERC-20 che sono stati emessi e venduti tramite ICO dal 2017. A rigor di termini, i token non sono criptovalute come Bitcoin o Ethereum, ma unità di valore trasferibili emesse su una blockchain. Esistono diverse classificazioni dei token in base alle varie caratteristiche dei token. La classificazione principale utilizza la funzionalità per dividere i token in token utility e token security. I token utility generalmente rappresentano l'accesso a un servizio o possono funzionare come mezzo di scambio all'interno di un ecosistema.

Tokenize

Livello: intermedio

Argomento: finanza

Il processo mediante il quale le risorse del mondo reale sono trasformate in token , spesso successivamente in grado di offrire la proprietà di parti di questa risorsa a proprietari diversi.

Tokenomic

Livello: intermedio

Argomento: tecnologia

La parola tokenomics è una combinazione di token ed "economia", e qui il termine token può significare una criptovaluta nativa o un token emesso su una piattaforma ad esempio da uno smart contract.

"Economia" si riferisce alla progettazione del token, comprese le eventuali misure in atto per aiutare a gestire l'inflazione, la deflazione, l'offerta e la domanda. Alcuni di questi metodi, come limitare l'offerta di token e controllare la velocità con cui vengono emessi nuovi token, sono discussi sopra.

Con Tokenomic si intendono le caratteristiche dell'economia di un dato token che governano le dinamiche del token e il motivo per cui questo token possa essere utile, guadagnare o perdere valore, cioè qual è il modo e il rapporto di distribuzione dei token, l'assegnazione, l'uso, i meccanismi incorporati, come burning.
La comprensione della tokenomic combina teoria dei giochi, matematica ed economia tradizionale. Il suo obiettivo è risolvere i problemi di coordinamento e incentivazione tra i partecipanti in una rete decentralizzata.

Tor

Livello: intermedio

Argomento: tecnologia

Tor è un protocollo di rete e un software gratuito per abilitare la comunicazione anonima.

Il nome deriva da un acronimo per il nome del progetto software originale "The Onion Router".

Consiste in una rete di relè volontari per nascondere la posizione e l'utilizzo degli utenti.

Total Supply

Livello: intermedio

Argomento: economia

Il total supply, in italiano fornitura o offerta totale, indica la quantità totale di bitcoin, coin e token nel caso di altre criptovalute esistenti.

A volte total supply viene utilizzato con lo stesso signficato di max supply, anche se hanno un significato leggermente diverso.

La Circulating supply, o current supply, indica invece la quantità di coin esistenti al momento, al netto di quelli che sono stati bruciati in modo verificabile.

I 21 Milioni di Bitcoin Nel caso di bitcoin la max supply è di 21 milioni di bitcoin, e si dovrebbe arrivare a questa quantità di bitcoin minati in totale circa nel 2140.

Come è stato determinato tale valore? Ci sono diverse ipotesi.
Tra queste, c'è la testimonianza di Ray Dillinger, sencondo il quale con Satoshi Nakamoto e Hal Finney discutevano sul total supply.
Allora, nel 2008, il valore globale della massa monetaria M1 o liquidità primaria (banconote e monete di tutte le valute fisiche in circolazione, depositi bancari e altre forme di denaro altamente liquide) secondo il report della CIA era circa 21 mila miliardi di dollari, ovvero 21 con 12 zeri.
Finney osservò allora che la divisione più piccola del dollaro era il centesimo, e quindi l'M1 mondiale in centesimi di dollaro era 21 con 14 zeri dopo, che corrisponde ai 21 000 000 000 000 00 di unità più piccole di bitcoin (ovvero satoshi che però allora non si chiamavano ancora così)

TPS

Acronimo di: Transactions Per Second

Transazioni al secondo

Livello: intermedio

Argomento: tecnologia

Nel contesto delle blockchain, le transazioni al secondo (TPS) si riferiscono al numero di transazioni che una rete è in grado di elaborare ogni secondo.

Le TPS medie approssimativo della blockchain di Bitcoin è generalmente di circa 5 - anche se questo può variare a volte.
Il 23 aprile 2024 ci sono state oltre 920 mila transazioni in un giorno, con una media nella giornata di oltre 10 TPS.

Lo sviluppo di tecnologie che aumentano il tasso di transazione delle blockchain è stata un'importante area di ricerca nel corso degli anni. Queste reti decentralizzate pongono sfide completamente nuove in termini di capacità di scalare per l'aumento della domanda.

Questa sfida non riguarda solo l'aumento del TPS. I sistemi basati su database centralizzati sono già in grado di gestire migliaia di transazioni ogni secondo. VISA, per esempio, gestisce circa 1.500-2000 transazioni ogni secondo. Quindi perché non usare semplicemente queste soluzioni? Beh, il problema principale è che Bitcoin, Ethereum e altre blockchain mirano a competere con questo mantenendo un alto grado di decentralizzazione. La decentralizzazione ha un costo in termini di prestazioni, e richiede nuovi approcci per essere gestita e gestire temi quali la sicurezza.

È importante notare che se una blockchain ha un valore alto di TPS, non è necessariamente superiore ad altre blockchain con TPS inferiore. Molti progetti

di blockchain si vantano dei loro alti numeri TPS. Tuttavia, è quasi certo che tali prestazioni sono state ottenute sacrificando altri aspetti importanti della rete. Per esempio, in qualsiasi momento, Bitcoin ha migliaia di nodi distribuiti in tutto il mondo che eseguono il software Bitcoin. Una blockchain con solo 10-20 nodi potrebbe facilmente superare Bitcoin, ma difficilmente potrebbe essere chiamata decentralizzata o anche distribuita.

Bitcoin attraverso l'uso di soluzioni quali Lightning Network, ha un potenziale di un numero illimitato di TPS.

trampoline

Livello: avanzato

Argomento: tecnologia

Trampoline è una tecnica per i pagamenti su Lightning Network che consente al pagatore di instradare il pagamento verso un nodo intermedio che può selezionare il resto del percorso per il ricevitore finale, ovvero di delegare i segmenti del percorso di routing a nodi intermedi.

Trampoline payment sono un nuovo modo suggerito di outsourcing che mira a far sì che i lite client esternalizzino il calcolo del percorso ai nodi trampoline, nodi con una maggiore memoria, larghezza di banda e potenza di calcolo.
Questo è vantaggioso per i lightweight client di Lightning Network che non sono in grado di monitorare l'intera rete perché spesso sono offline o eseguiti su hardware mobile meno potente.

L'utilizzo di un singolo nodo trampoline rivelerà necessariamente la destinazione del pagamento, il che è negativo per la privacy.
Pertanto, il pagante può richiedere che il pagamento venga instradato attraverso più nodi trampoline. In questo modo, nessuno di essi sa se sta instradando il pagamento verso il destinatario finale o solo un altro nodo trampoline intermedio.

Sebbene consentire ai nodi trampoline di selezionare parte del percorso probabilmente richieda il pagamento di fee di instradamento più elevate, ciò consente che il pagante non deve sapere come instradare i pagamenti verso qualsiasi nodo arbitrario: è sufficiente che il pagante sappia come instradare un pagamento verso qualsiasi nodo compatibile con trampoline.

Le fee per i pagamenti Trampoline saranno più alte rispetto a quelle di un trasferimento Lightning standard perché il nodo trampoline deve essere in grado di inoltrare il pagamento verso qualsiasi nodo nella rete e riscuotere una piccola tariffa per il suo lavoro di calcolo del percorso, o pathfinding.

Il pagamento trampoline può attraversare uno o più hop a seconda del percorso che segue, e più lungo è il tragitto, maggiore saranno le fee da pagare. Pertanto, sebbene aggiunga comodità agli utenti di Lightning, comporta maggiori costi.

Transaction Malleability

Malleabilità della transazione

Livello: avanzato

Argomento: tecnologia

La Transaction Malleability è un problema per sviluppatori e utenti che desiderano fare riferimento a una transazione precedente in una nuova transazione di spesa prima che la transazione precedente sia stata confermata sulla blockchain. Questo problema sorge perché, per spendere i bitcoin creati da una transazione precedente, la transazione di spesa deve fare riferimento al txid della transazione precedente. Se questo txid può cambiare, il riferimento fallirà e la transazione di spesa sarà resa non valida.

In particolare, la malleabilità delle transazioni è stata un problema che ha impedito l'adozione del Lightning Network, che si basa sullo scambio di transazioni Bitcoin non confermate.

Una transazione può essere "malleata" in due modi:

- innanzitutto, dopo che una transazione è stata firmata, è possibile aggiungere ulteriori dati a uno ScriptSig, la parte della transazione che contiene la firma e altri dati utilizzati per sbloccare i bitcoin;
- in secondo luogo, è possibile modificare la firma stessa, contenuta all'interno di ScriptSig. Queste opzioni sono entrambe possibili perché una firma non può firmare se stessa e quindi non può rendersi immutabile. Poiché lo ScriptSig e le firme che contiene fanno parte della preimmagine txid, se vengono modificati, il txid cambierà.

Come SegWit ha risolto la malleabilità delle transazioni:

SegWit elimina questa possibilità rimuovendo tutti i dati dallo ScriptSig.
Ciò si ottiene spostando i dati ScriptSig, solitamente firme e chiavi pubbliche, nel Witness, una nuova parte delle transazioni SegWit che non viene sottoposta ad hashing per calcolare il txid.
Gli input di ScriptSig per SegWit vengono quindi resi immutabili dopo la firma e i dati necessari per sbloccare bitcoin, che non sono immutabili, sono contenuti nel Witness. Ciò significa che lo ScriptSig non può essere modificato, e quindi il txid non può essere modificato senza invalidare l'intera transazione.

Transaction pinning

Livello: avanzato

Argomento: tecnologia

Il Transaction pinning, pinning delle transazioni, è un metodo per rendere proibitivo l'aumento delle fee, abusando delle protezioni dei nodi contro gli attacchi che possono sprecare larghezza di banda, CPU e memoria. Questo

può rendere più difficile la gestione delle commissioni nei protocolli di contratto multiparte (come Lightning Network).

I nodi come Bitcoin Core che permettono di sostituire le transazioni con RBF, o di impacchettarle con transazioni figlio a tariffa più alta CPFP, pongono restrizioni su tali sostituzioni per prevenire vari attacchi DoS. Tuttavia, quando due o più persone hanno la possibilità di effettuare il fee bump di una transazione, questo rende possibile che uno di loro possa bloccare, pin, la propria versione di una transazione a uno dei limiti e impedire agli altri partecipanti di utilizzare il fee bump.

Alcuni dei limiti che possono essere abusati per consentire il pinning delle transazioni sono:

- La regola #3 del BIP125 RBF richiede che una transazione sostitutiva paghi una commissione assoluta (non solo feerate) più alta della somma delle commissioni pagate dalla transazione sostituita e da tutti i suoi figli. Ciò può consentire a un aggressore di allegare una transazione di grandi dimensioni e a bassa feerate alla transazione che vuole bloccare, costringendo qualsiasi aumento delle commissioni a pagare per la sostituzione della transazione figlia di grandi dimensioni. Ad esempio, con le impostazioni predefinite di Bitcoin Core del 2019, un aggressore può richiedere a un partecipante onesto di pagare un minimo di 0,001 BTC per effettuare il fee bump di una transazione (o anche importi maggiori in alcuni casi).
- Le limitazioni sulla dimensione massima dei pacchetti impediscono l'uso di CPFP se una transazione ha più di 101.000 vbyte di figli o altri discendenti in una mempool, o ha più di 25 discendenti o antenati. Ciò può consentire a un aggressore di bloccare completamente il fee bumping creando la quantità massima di transazioni figlio. Se l'attaccante deve creare tali transazioni per altri motivi (ad esempio perché gestisce un servizio a pagamento per gli utenti), questo attacco può essere gratuito. Per alcuni protocolli di contratti a due parti (come l'attuale Lightning Network), questo problema è mitigato dal CPFP carve out.

Transaction replacement

Sostituzione della transazione

Livello: avanzato

Argomento: tecnologia

Transaction Replacement, o sostituzione della transazione, a volte indicata più porecisamente come unconfirmed transaction replacement si riferisce alla possibilità di sostituzione di una transazione nella mempool, ovvero non ancora confermata nella blockchain, con una nuova transazione.

Ci sono diversi motivi per si può voler sostituire o meglio aggiornare le transazioni: per aumentare le loro fee, comprimere più transazioni in una sola,

creare coinjoin in background (per migliorare la privacy) o eseguire una serie di altre azioni utili.

Questa sostituzione attualmente può avvenire attraverso comportamenti ben definiti, quali RBF Replace-by-fee.

La sostituzione delle transazioni non confermate era una caratteristica della prima versione del client bitcoin scritto da Satoshi Nakamoto, si basava sul valore nSequence della transazione, il che significa che era possibile emettere una nuova transazione e i nodi l'accettavano se l'ID della sequenza era più alto sostituendo la transazione esistente nella mempool. Questa funzione è stata rimossa dal client nella versione 0.3.12 (settembre 2010). Satoshi Nakamoto ha commentato questa rimozione: "Disabilita la funzione di sostituzione per ora", perché era possibile per un aggressore utilizzare tutta la larghezza di banda tra i full node con un costo minimo per se stesso, creando una vulnerabilità denial-of-service.

Tale funzionalità è rimasta assente nel client principale per molti anni da allora.

La regola generalmente accettata dalla rete (miner, nodi non mining) per molti anni è stata la FSS First-Seen-Safe, ovvero che i nodi, quando ricevevano le transazioni, controllavano se nella mempool c'era già un'altra transazione che stava spendendo lo stesso UTXO, e nel caso in cui tale transazione fosse stata trovata, la nuova veniva rifiutata.

I miner possono usare versioni personalizzate del software Bitcoin, e quando un miner confeziona un nuovo blocco ha la libertà di selezionare quali transazioni inserire, e non erano incentivati a seguire questa convenzione e ad accettare una sostituzione, e potevano addirittura essere incentivati a violare questa convenzione se una versione precedente di una transazione pagava una fee più alta.

Questi due fattori hanno impedito per alcuni anni che la Transaction Replacement fosse ripristinata su Bitcoin Core, ma nel 2013 Peter Todd ha proposto di imporre alle Transaction Replacement di pagare fee rigorosamente maggiori e di richiedere che la sostituzione aumenti la fee almeno del minimo richiesto per trasmettere una nuova transazione. In questo modo si eliminavano i problemi di denial of service e di compatibilità degli incentivi.

Il lavoro originale di Peter Todd è andato oltre e ha portato la compatibilità degli incentivi alla sua logica conclusione, ragionando sul fatto che con miner anonimi, effimeri e autoselezionati l'unico comportamento su cui si può davvero contare è l'incentivo economico e quindi la sostituzione con fee più alte. La preferenza per fee più elevate può anche rendere possibile ai nodi di convergere su un insieme di transazioni nella mempool in base alle fee in modo che non sia possibile per i nodi accettare solo la prima versione che viene vista di una transazione.

Per questi motivi e poiché un sistema che si comporta in modi prevedibili è più sicuro e protetto di un sistema che si comporta in "modi imprevedibili ma mediamente migliori", ha proposto che la sostituzione avvenga per tutte le transazioni.

Ha anche proposto un protocollo per rimuovere i guadagni economici derivanti dal Double Spend in un modo fortemente compatibile con gli incentivi, chiamato *replacement scorched earth* (terra bruciata), in cui se qualcuno tenta di spendere due volte, si spendono tutti i fondi per le fee in modo che l'attaccante non li ottenga. (Ma questo è il tipo di proposta che solo un teorico dei giochi potrebbe amare).

Dopo la proposta di Peter Todd, alcuni produttori di wallet hanno chiesto con forza un RBF opt-in, in quanto avevano bisogno di un modo ragionevole per gestire le fee e vedevano nell'RBF opt-in un buon modo per farlo, motivo per cui la proposta è stata cambiata in modo da corrispondere al comportamento opt-in originale di Satoshi.

A partire da Bitcoin Core 0.12.0 (rilasciata nel febbraio 2016), è diventato ampiamente disponibile il tipo di transaction replaceability RBF replace-by-fee.

Dalla versione 0.16.0 (febbraio 2018) di Bitcoin Core le transazioni RBF sono diventate un comportamento predefinito (da opt-in a opt-out) e la Transaction replacement, la sostituzione delle transazioni è diventata uno standard de facto sulla rete. Tale cambiamento è stato collegato al limite di 1Mb del blocco e si è reso necessario uno strumento per gli utenti per sostituire le transazioni bloccate.

L'attributo più controverso di RBF è che permetteva di inviare fondi a indirizzi assolutamente diversi tramite la modalità definità Full RBF, il che significa praticamente che gli utenti possono tentare un double spend tramite un Race Attack con un software standard.

E la polemica si è accesa ulteriormente con l'annuncio che la versione 24.0 di Bitcoin Core avrà Full-RBF abilitata di default.

Transaction Weight

Peso della transazione

Livello: avanzato

Argomento: tecnologia

La Transaction Weight o Peso della transazione è una metrica per misurare la *dimensione* di una transazione.

Con l'introduzione di SegWit, le transazioni hanno ricevuto una nuova unità di misura chiamata Weight o peso.

Questa unità di misura dà alla parte di convalida di una transazione (i dati della firma) uno sconto, in modo che non occupi tanto "spazio" all'interno di un blocco. In altre parole, i dati della firma sono meno costosi del resto dei dati della transazione.

Il weight o peso di una transazione viene calcolato moltiplicando la dimensione (in byte) delle diverse parti dei dati della transazione per diversi valori:

Data	Moltiplicatore
Version	x4
Marker	x1
Flag	x1
Input Count	x4
Input	x4
Output Count	x4
Output	x4
Witness	x1
Locktime	x4

Il fattore 4 contribuisce a creare un maggiore equilibrio tra il costo di creazione di un output e il costo di spesa di un output.

Travel rule

Regola di viaggio

Livello: avanzato

Argomento: politica

La Travel Rule è un obbligo vincolante richiesto dal FAFT/GAFI, un organismo intergovernativo indipendente che sviluppa e promuove l'AML (antiriciclaggio) e il KYC (Know Your Customer), che ha pubblicato indicazioni su come i suoi 37 membri dovrebbero regolare gli scambi di criptovalute, anche se la maggior parte delle giurisdizioni non l'ha effettivamente attuata. La Svizzera, tramite la sua autorità di vigilanza FINMA, ha pubblicato una guida che copre la Travel Rule nel 2019 che è entrata in vigore il 1° gennaio 2020.

La Travel Rule è un insieme di linee guida che richiedono ai prestatori di servizi finanziari di trasmettere e conservare informazioni sulle transazioni finanziarie, comprese quelle effettuate tramite criptovaluta.

Viene applicato con il dichiarato intento di prevenire il riciclaggio di denaro e il finanziamento del terrorismo.

A seguito dell'incremento degli investimenti in criptovalute e Bitcoin negli ultimi anni, i regolatori stanno ora mettendo gli occhi su questa parte dinamica e in rapida evoluzione del settore dei servizi finanziari.

Mentre molti nel settore accolgono con favore la supervisione normativa, in quanto fornisce chiarezza e certezza sia per gli investitori che per gli operatori, un pezzo di guida - la raccomandazione 16 - ha causato una significativa controversia. La cosiddetta travel rule richiede l'obbligo di ottenere, detenere e

trasmettere le informazioni richieste sull'originatore e sul beneficiario al fine di identificare e segnalare le transazioni sospette, monitorare la disponibilità delle informazioni, intraprendere azioni di congelamento e vietare le transazioni con persone ed entità designate.

Il FATF non si riferisce a questa raccomandazione come travel rule, ma ha una sorprendente somiglianza con una precedente regola del BSA Bank Secrecy Act [31 CFR 103.33(g)] con quel nome, che richiede a tutte le istituzioni finanziarie di passare certe informazioni all'istituzione finanziaria di controllo, in certe trasmissioni di fondi che coinvolgono più di una istituzione finanziaria.

Per poter implementare la Travel rule nei loro sistemi, diversi operatori del settore hanno aderito a TRUST Group, che ha predisposto una soluzione per fornire la conformità a questo requisito.

TRUC

Acronimo di: Topologically Restricted Until Confirmation

Livello: avanzato

Argomento: tecnologia

Le transazioni "Topologically Restricted Until Confirmation" (TRUC) in Bitcoin sono una proposta per migliorare l'affidabilità e la prevedibilità delle transazioni, attivate con la versione 28.0 di Bitcoin Core pubblicata a ottobre 2024.

Uno degli casi d'uso più comuni per le transazioni Truc, riguarda i canali lightning network: quando due soggetti aprono un canale lightning, creano e si scambiano delle transazioni che possono essere pubblicate anche molto tempo dopo la loro creazione, e quindi è difficile stabilire quali possano essere le fee più adatte, per evitare che le fee siano troppo basse e la transazione non venga confermata, o che siano inutilmente costose; tramite TRUC diventa possibile inserire delle fee basse, per poi stabilire le fee effettive al momento in cui si vuole pubblicare la transazione tramite una transazione CPFP.

È una politica per le transazioni Bitcoin con numero di versione impostato su 3, introdotta con il BIP 431. Questa politica impone restrizioni sulle transazioni non confermate, limitando l'utilizzo di output non confermati e consentendo l'evizione di una transazione discendente precedente se viene presentata una nuova più compatibile dal punto di vista degli incentivi. Inoltre, stabilisce una dimensione massima per le transazioni di 10,000vB. Queste regole facilitano la valutazione della compatibilità degli incentivi per l'accettazione o la sostituzione delle transazioni TRUC, migliorando l'affidabilità delle operazioni di "fee-bumping" e massimizzando i profitti per il nodo.

Ecco come funzionano:

- **Limitazioni sulla spesa di output non confermati**: Una transazione TRUC impone restrizioni su come gli output (le "monete" in uscita) possono essere utilizzati finché la transazione stessa non viene confermata. Ciò significa che gli output TRUC non possono essere spesi immediatamente in un'altra transazione.
- **Maggiore affidabilità del fee bumping**: Il "fee bumping" è una tecnica usata per aumentare la fee di una transazione in attesa di conferma, in modo che venga elaborata dai miner con maggiore priorità. Le transazioni TRUC mirano a rendere il fee bumping più affidabile, garantendo che le transazioni con fee più alta vengano effettivamente incluse prima di quelle con fee più bassa.
- **Vantaggi per i nodi**: Le transazioni TRUC semplificano per i nodi della rete Bitcoin la valutazione della validità e dell'incentivo a processare la transazione. Questo perché le restrizioni sugli output non confermati rendono più prevedibili le conseguenze dell'accettazione o della sostituzione di una transazione TRUC.

Stato attuale: La policy per le transazioni Opt-in TRUC (nota anche come policy per le transazioni v3) è disponibile per l'utilizzo solo sulle reti di test con l'opzione -acceptnonstdtxn=1.
Impostando il numero di versione della transazione a 3, le transazioni TRUC richiedono l'applicazione di limiti alla spesa dei propri output non confermati. Queste restrizioni semplificano la valutazione della compatibilità degli incentivi per l'accettazione o la sostituzione di transazioni TRUC, garantendo così che eventuali sostituzioni siano più redditizie per il nodo e rendendo l'aumento delle commissioni (fee bumping) più affidabile. Le transazioni TRUC sono attualmente considerate non standard e possono essere utilizzate solo su reti di test in cui le regole di standardness sono allentate o disabilitate (ad esempio con -acceptnonstdtxn=1).

Vantaggi potenziali:

- **Maggiore affidabilità**: Fee bumping più efficace: Il fee bumping potrebbe diventare più affidabile e prevedibile con le transazioni TRUC.
- **Migliore scalabilità**: Le transazioni TRUC potrebbero contribuire a migliorare la scalabilità della rete Bitcoin a lungo termine.

TRUST Group

Acronimo di: Travel Rule Universal Solution Technology

Livello: avanzato

Argomento: legale

Trust (che come parola inglese significa anche "fiducia") è l'acronimo di Travel Rule Universal Solution Technology, è una soluzione alla quale aderiscono diversi

operatori del settore delle criptovalute, in particolare Exchange e in generale definiti come VASP, progettata per soddisfare un requisito noto come Travel rule.

La Travel Rule impone agli istituti finanziari di condividere alcune informazioni di base sui propri clienti quando inviano fondi superiori a un determinato importo a un altro istituto finanziario. I CEX (come altri istituti finanziari) devono soddisfare questa regola, che è stata scritta prima ancora che esistessero le criptovalute.

TRUST mira a fornire una conformità completa in tutto il settore delle criptovalute. La portata della Travel Rule si sta espandendo a livello internazionale. TRUST si concentra sull'espansione in diverse giurisdizioni.
I membri di TRUST attualmente includono una vasta gamma di Exchange, intermediari, custodi e fornitori di wallet tra i leader del settore.

PoAO, Proof of address ownership TRUST include un meccanismo PoAO, Proof of address ownership, Prova della proprietà dell'indirizzo, che consente per l'exchange ricevente di dimostrare di essere il proprietario dell'indirizzo crittografico ricevente delle cripto prima che le informazioni del cliente vengano inviate.

La soluzione TRUST incorpora due componenti separati per affrontare la Travel rule:

- un bulletin board centralizzato utilizzato per identificare il controparte corretto, consentendo a un VASP Originante di identificare un VASP Beneficiario; e
- un canale P2P crittografato per trasferire in modo sicuro i dati necessari alla Travel rule dal VASP Originante al VASP Beneficiario.

Questi i passaggi che vengono effettuati con Trust:

- Il VASP Beneficiario fornisce un indirizzo di deposito di criptovaluta al cliente destinatario. Il VASP Beneficiario fa l'hash e registra gli indirizzi di deposito di criptovaluta sul bulletin board TRUST come uno che possiedono, inclusi i dati di proprietà dell'indirizzo.
- Il cliente beneficiario fornisce l'indirizzo di deposito al cliente Originante.
- Il cliente Originante fornisce l'indirizzo del beneficiario al VASP Originante.
- Se una transazione è superiore a $3000, il VASP Originante pubblica l'indirizzo del beneficiario sul bulletin board del Travel Rule WG degli Stati Uniti.
- Il VASP Beneficiario risponde privatamente al VASP Originante, riconoscendo che l'indirizzo è loro.
- Invia la transazione Bitcoin o Ethereum sottostante.
- Il VASP Originante trasmette i dati PII e l'hash della transazione al VASP Beneficiario attraverso un metodo peer-to-peer.

Ogni VASP che utilizza TRUST fornisce un endpoint API simile a TRP. Tuttavia, TRUST aggiunge un bulletin board centralizzato per risolvere il problema della "scoperta", identificando quale VASP si trova dietro un indirizzo. Il bulletin board mostra un indirizzo del wallet e il VASP Originante che tenta di verificarlo. Il VASP Beneficiario risponde quindi privatamente per rivendicare la transazione.

Trustless

Livello: base

Argomento: tecnologia

Una proprietà della blockchain, in cui i partecipanti non hanno bisogno di fidarsi di nessun altro partecipante o di un soggetto terzo fiduciario affinché le transazioni vengano considerate affidabili, poiché le regole del protocollo impediscono che un partecipante possa effettuare operazioni non valide.

Tumbler

Livello: intermedio

Argomento: finanza

Un tumbler, noto anche come mixer o mixing service, è un servizio che mescola le transazioni Bitcoin di diversi utenti, rendendo più difficile rintracciare la fonte dei fondi.
Tramite un tumbler l'utente invia dei Bitcoin al servizio, che li mescola con Bitcoin provenienti da altri utenti. Il servizio quindi invia i Bitcoin mescolati all'utente, e in questo modo diventa difficile identificare da quale account provengano i fondi.

Nonostante spesso i tumbler vengano associati ad attività illegali quali riciclaggio di denaro, in realtà sono un importante strumento che consente di garantire la privacy, per attività perfettamente legali come l'acquisto di beni o servizi in modo anonimo, o attività umanitarie quali donazioni a soggetti perseguitati dai governi dei propri paesi.

Nella maggior parte dei paesi non esiste una legge che rende illegale l'uso dei tumbler di per se, ma può essere illegale il fatto di usarli per compiere crimini o attività illegali quali il riciclaggio di denaro.

Ad esempio il Dipartimento del Tesoro degli Stati Uniti ha di fatto vietato per tutti i cittadini americani l'utilizzo di Tornado Cash, una delle principali piattaforme di mixing attiva nell'ecosistema Ethereum.

Turing-Complete

Turing completo

Livello: avanzato

Argomento: tecnologia

Turing Complete, in italiano Turing equivalente o Turing completo, si riferisce a una macchina o a un sistema informatico che, in teoria, con tempo e memoria sufficienti insieme alle istruzioni necessarie, può risolvere qualsiasi problema computazionale, non importa quanto complesso.

Nel caso delle criptovalute è stato inizialmente utilizzato per distinguere le capacità degli script bitcoin, che generalmente non sono considerati turing complete, rispetto agli smart contract Ethereum che sono considerati turing complete.

L'idea che Bitcoin non sia Turing complete non è universalmente accettata, ed esistono delle dimostrazioni empiriche che una qualsiasi macchina di Turing possa essere simulata su bitcoin. Per alcuni, il fatto che Bitcoin non sia Turing complete è considerata una qualità positiva, poiché ne garantirebbe stabilità e minore possibilità che negli script possano essere introdotti dei bug.

Il problema principale della Turing-completness è che un computer non è in grado di distinguere tra un programma che è computabile e uno che non lo è fino a che non procede con l'esecuzione; se uno script non computabile venisse inserito dentro una transazione Bitcoin, tutti i nodi che proverebbero a validarla rimarrebbero bloccati, paralizzando di fatto il network. Per questo motivo su Bitcoin si è sempre preferito evitare la Turing-completness in modo da prevenire loop e script di cui non è possibile completare l'esecuzione.

Il principale problema legato alla completezza di Turing è che un computer non può distinguere tra un programma computabile e uno non computabile fino a quando non esegue effettivamente il processo. Se uno script non computabile fosse inserito all'interno di una transazione Bitcoin, tutti i nodi che cercano di convalidarla rimarrebbero bloccati, causando di fatto il blocco dell'intera rete. Per questa ragione, su Bitcoin è sempre stato preferibile evitare la completezza di Turing al fine di prevenire cicli e script che non possono essere eseguiti completamente.

TX

Acronimo di: Transaction

Transazione

Livello: base

Argomento: tecnologia

La transazione è un trasferimento di valore di criptovaluta che viene trasmesso alla rete, raccolta in blocchi e inserita nella blockchain. Una transazione in genere fa riferimento agli output non spesi generati da transazioni precedenti chiamati UTXO come nuovi input di transazione.

Le transazioni sono strutture di dati utilizzate da Bitcoin per trasferire bitcoin da un indirizzo all'altro. Diverse migliaia di transazioni vengono aggregate in un blocco, che viene poi registrato (minato) sulla blockchain. La prima transazione in ogni blocco, chiamata transazione coinbase, genera nuovi bitcoin.

Una transazione Bitcoin non contiene un indirizzo di provenienza, ma un insieme di UTXO o input non spesi, e la transazione contiene gli script, che sono puzzle crittografici e soluzioni degli stessi che nella transazione vengono risolti e quindi gli input vengono spesi e i loro importi trasferiti a nuovi UTXO generati dalla transazione.

Ogni transazione è autenticata da un mittente con la soluzione di un precedente puzzle crittografico memorizzato come script, questa soluzione è chiamata unlocking script. La nuova transazione viene bloccata per il destinatario con un nuovo puzzle crittografico, anch'esso memorizzato come script e chiamato locking script. Questi script, che bloccano e sbloccano le transazioni, sono scritti in Bitcoin Script

È possibile comprendere Bitcoin conoscendo come funzionano le transazioni, che possono avere più ingressi e più uscite.

Non ci sono coin o monete che si muovono da un indirizzo all'altro in bitcoin perché ogni transazione "distrugge" tutti gli input e crea nuovi output. Se si vuole pensare all'analogia con le monete - cioè se si considera ogni UTXO come una moneta di dimensioni diverse - si può pensare a ogni transazione come a un processo di fusione. Tutti gli input vengono liquefatti in una grande fornace e come output vengono create nuove monete.

Una transazione Bitcoin standard è composta da una versione, un elenco di input, un elenco di output, e un lock_time. Più precisamente ha 6 campi dati:

- version number
- numero di ingressi
- lista degli input
- numero di output
- lista degli output
- Lock_time

txid

Acronimo di: Transaction ID

identificativo della transazione

Livello: avanzato

Argomento: tecnologia

Un txid è una stringa di lettere e numeri che identifica una transazione specifica sulla blockchain.

La stringa è semplicemente il doppio hash SHA-256 di una transazione serializzata.

Questo hash può essere utilizzato per cercare una transazione su un nodo o su un Block Explorer.

Quando si firma una transazione, è infatti il txid che viene firmato. La firma del txid garantisce che se una qualsiasi parte della transazione cambia, l'ID della transazione cambia e la firma viene resa non valida.

Tecnicamente, un txid non è sempre un hash dell'intera transazione. Poiché una firma non può firmare da sola, le firme non sono incluse nel txid e quindi le firme possono essere modificate dopo la loro creazione, a volte senza essere invalidate.

Prima di SegWit, questo consentiva a un txid di cambiare dopo la firma della transazione, un problema chiamato Transaction Malleability; con l'introduzione di SegWit per differenziare il formato particolare del txid legacy con quello segwit, viene utilizzato il termine wtxid.

UASF

Acronimo di: User-Activated Soft Fork

Soft Fork attivato dall'utente

Livello: avanzato

Argomento: politica

Un UASF, acronimo di User Activated Soft Fork in italiano Soft Fork Attivato dagli Utenti, è un tipo di aggiornamento di un protocollo blockchain, in cui gli utenti della rete prendono l'iniziativa di implementare una modifica al software senza il sostegno esplicito dei miner.
Questo approccio è spesso utilizzato quando una parte significativa della comunità desidera introdurre un cambiamento nel protocollo, ma i miner non sono d'accordo o non si attivano per adottare la modifica.

L'adozione da parte degli utenti crea comunque le condizioni affinché anche i miner, in un momento futuro, laddove ci sia una grande adozione siano portati ad aggiornarsi adeguandosi al cambiamento del protocollo.
Essendo un soft fork, le nuove regole sono retrocompatibili con le vecchie regole, il che significa che i nodi che non hanno aggiornato il loro software possono continuare a partecipare alla rete, con un opt-in per le parti interessate alle nuove caratteristiche del protocollo, anche se in un momento futuro, i miner

potrebbero essere a rischio di creare blocchi non validi. Inoltre, un soft fork attivato dall'utente è uno che è prevalentemente guidato dall'attività dell'utente, non dai miner o da altre parti, e che i minatori saranno generalmente costretti a seguire.

Un esempio di un UASF è il BIP 148, un UASF che promuove la distribuzione di Segregated Witness o SegWit, un protocollo che cambia il modo in cui le firme digitali sono gestite in bitcoin. BIP 148 è stato creato per trovare un modo più "morbido" per implementare Segregated Witness - per incoraggiare i miner ad aggiornare il loro software e utilizzare SegWit.

Molti di questi tipi di cambiamenti sono attualmente in discussione nella comunità bitcoin, con iniziative concorrenti che determinano il valore e l'uso del bitcoin negli anni futuri.

UIF

Unità di informazione finanziaria

Livello: intermedio

Argomento: legale

L'UIF, l'Unità di informazione finanziaria, è un'autorità amministrativa indipendente istituita presso la Banca d'Italia. È preposta alla ricezione, analisi e scambio di informazioni, anche su base internazionale, relative a operazioni sospette di riciclaggio e di finanziamento del terrorismo.

Nel settore delle criptovalute, l'UIF svolge un ruolo importante nel contrasto a questi reati. In particolare, l'UIF riceve segnalazioni di operazioni sospette da VASP, i prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale, come gli exchange di criptovalute.

L'UIF analizza queste segnalazioni per verificare se possano essere riconducibili a operazioni di riciclaggio o di finanziamento del terrorismo. In caso affermativo, l'UIF trasmette le segnalazioni alle autorità competenti, quali la Guardia di Finanza e la Direzione Nazionale Antimafia e Antiterrorismo.

L'UIF svolge anche un ruolo di sensibilizzazione e formazione nei confronti dei VASP, al fine di aiutarli a individuare e segnalare operazioni sospette.

Ecco alcuni esempi di operazioni sospette che possono essere segnalate all'UIF:

- Operazioni di importo elevato o insolito;
- Operazioni effettuate da soggetti sconosciuti o poco conosciuti;
- Operazioni effettuate per conto di terzi;
- Operazioni che non hanno una giustificazione economica o finanziaria plausibile.

Segnalare un'operazione sospetta è un dovere di legge per i VASP.

L'UIF spesso collabora con altre UIF a livello internazionale e con organizzazioni come il FATF, Gruppo d'azione finanziaria, per condividere informazioni e sviluppare linee guida internazionali per la regolamentazione delle criptovalute.

Unhosted Wallet

Livello: intermedio

Argomento: legale

Il termine "*unhosted wallet*", letteralmente "*wallet non ospitato*", viene usato in modo negativo dai legislatori, ad esempio dal regolamento MiCA per indicare i wallet non custodial, o non fiduciari. Un wallet unhosted è un wallet che non è ospitato su un server di un fornitore di servizi finanziari come un istituto finanziario o un fornitore di servizi di credito o un exchange centralizzato.

In realtà un unhosted wallet o wallet non fiduciario ha il vantaggio che non c'è nessun terzo che può accedere alle tue informazioni o modificarle, ad esempio sequestrando i fondi o imponendo regole per ritirare i propri fondi. Ciò significa che non c'è nessun servizio di terze parti che detiene le tue informazioni o i tuoi fondi, e solo tu puoi muovere i tuoi fondi e nessuno altro.

Chiamare un normale wallet bitcoin "unhosted" dà in primo luogo l'impressione che dovrebbe essere "ospitato"; che manca qualcosa a come dovrebbe essere. In realtà, è vero il contrario: chi può accedere ai vostri fondi? Chi può bloccare il vostro conto? Chi li controlla? Un "hosted wallet" è il wallet di qualcun altro: il denaro detenuto e controllato da altri può essere e sarà manipolato.

I wallet Bitcoin dovrebbero essere non ospitati o, per usare una parola che non è stata inventata da ai legislatori e ai regolatori probabilmente non piace: indipendenti. Lo scopo di Bitcoin è quello di portare la piena sovranità all'individuo e di eliminare ogni dipendenza da terze parti fidate. Niente governanti, niente padroni, niente host. Solo peer.

Invece di usare il termine "wallet non ospitato", ci si potrebbe riferire ai normali wallet Bitcoin come wallet indipendenti o wallet di libertà (nella comunità di Bitcoiner italiana si è diffuso il termine "non-custodial"). L'opposto di un wallet indipendente è un servizio di custodia, il che significa che avete un permesso, niente di più. Utilizzando un servizio di custodia, si distrugge ciò che principalmente rende prezioso Bitcoin. Si ritorna al modello di denaro autorizzato: un rapporto di debito tra padroni e schiavi, che è il sistema fiat da cui vogliamo allontanarci. Alcuni hanno tutto il potere, gli utenti non ne hanno alcuno.

Un servizio di custodia di questo tipo, un servizio che vogliono farvi chiamare "wallet ospitato" non è altro che un altro conto gestito da qualcuno che assomiglia molto ad una banca.

Un wallet dovrebbe essere self-hosted e questo non rappresenta un crimine. Tuttavia, non dovremmo pensare agli "host". Un wallet non ha bisogno di essere ospitato perché un wallet non è altro che una chiave - un'informazione privata

- combinata con un hardware o un software che consente di fare qualcosa con tale chiave, ad esempio ricavare indirizzi o firmare transazioni.

Lasciare che qualcun altro detenga le vostre chiavi distrugge tutti i vantaggi che il bitcoin porta con sé. Se ci si potesse fidare di altri con il nostro denaro, non avremmo avuto bisogno di Bitcoin.

Unicode

Livello: avanzato

Argomento: tecnologia

Unicode è uno standard internazionale di codifica dei caratteri che assegna un numero a ogni carattere, indipendentemente dalla piattaforma, dal programma o dalla lingua. Nato con l'obiettivo di fornire un sistema unificato per rappresentare testi di tutte le lingue scritte del mondo, Unicode supporta più di 150 sistemi di scrittura, inclusi alfabeti, ideogrammi, simboli matematici e pittogrammi moderni.

Lo standard Unicode fornisce una base per la rappresentazione di caratteri mediante diversi schemi di codifica, tra cui UTF-8, UTF-16 e UTF-32, che si differenziano per lunghezza e modalità di rappresentazione binaria dei caratteri. UTF-8 è la codifica più comunemente usata in applicazioni web e software, grazie alla sua compatibilità con ASCII e alla sua efficienza nel gestire testi prevalentemente in inglese.

Unicode e la codifica delle passphrase Bitcoin Nel contesto delle passphrase Bitcoin, in particolare nel sistema BIP-39, Unicode svolge un ruolo fondamentale nella generazione e gestione di mnemonic phrases (frasi mnemoniche). Queste frasi sono sequenze di parole leggibili dall'uomo che rappresentano una chiave privata in modo sicuro e recuperabile.

L'uso di Unicode garantisce che le frasi mnemoniche possano includere caratteri di lingue diverse e che le passphrase personalizzate siano rappresentate in modo standardizzato. Tuttavia, per evitare ambiguità nella codifica, è essenziale normalizzare i caratteri Unicode in una forma standard, che garantisca consistenza tra piattaforme e sistemi.

Varianti di normalizzazione Unicode: NFKD e NFC Le varianti di normalizzazione Unicode determinano come i caratteri composti e decomposizioni siano rappresentati in modo coerente. Queste forme sono critiche per applicazioni come la generazione di passphrase Bitcoin, dove anche la minima differenza nella rappresentazione può compromettere l'accesso ai fondi crittografici.

NFC (Normalization Form C) Questa è la forma utilizzata da (BIP 38)[bip-38-passphrase-protected-private-key.html].
Questa forma combina caratteri che possono essere rappresentati sia come

carattere base più segni diacritici separati, sia come carattere unico precomposto. Ad esempio, la lettera “é” (U+00E9) in NFC è rappresentata come un unico carattere precomposto.

NFKD (Normalization Form KD) Questa è la forma utilizzata da BIP-39.
In questa forma, i caratteri sono decomposti in caratteri base e segni diacritici separati. Ad esempio, “é” viene scomposto in “e” (U+0065) più il segno diacritico acuto (U+0301). Inoltre, NFKD considera anche l’equivalenza di compatibilità, trasformando simboli o legature in rappresentazioni canoniche equivalenti.

Implicazioni nella codifica Bitcoin L’uso improprio della normalizzazione Unicode nelle passphrase Bitcoin può portare a problemi di compatibilità tra wallet o, nei casi peggiori, all’impossibilità di recuperare i fondi.
Questo perchè caratteri che possono essere rappresentati visivamente identici, se sono codificati diversamente non vengono riconosciuti.

Esempio concreto:
Supponiamo che una passphrase contenga la lettera “é”. Questa lettera può essere rappresentata in Unicode in due modi:

Come un singolo carattere “é” (U+00E9)
Come la combinazione di “e” (U+0065) e accento acuto “‘” (U+0301)
Se la passphrase viene generata con la prima rappresentazione e il wallet utilizzato per il recupero si aspetta la seconda, la passphrase non verrà riconosciuta, nonostante appaia identica all’utente.

Per mitigare questo rischio è fortemente sconsigliato usare caratteri accentati o caratteri speciali nelle pass phrase.

Uniswap

Livello: intermedio

Argomento: tecnologia

Uniswap (UNI) è un exchange decentralizzato. Uniswap si basa su smart contract che facilitano lo scambio di token e forniscono la struttura di incentivi per i fornitori di liquidità per partecipare al sistema. Essendo uno dei primi market maker automatizzati (AMM) a essere attivo sulla rete Ethereum, Uniswap ha compiuto progressi significativi nel dimostrare che gli AMM possono essere uno strumento efficace per il trading di risorse digitali in modo decentralizzato e senza autorizzazione.

Unit of account

Unità di conto

Livello: base

Argomento: economia

L'unità di conto è un concetto economico che si riferisce a una misura standard del valore, utilizzata per confrontare i prezzi di beni e servizi. È una funzione essenziale del denaro, che è tradizionalmente considerato l'unità di conto più comune.

Un'unità di conto deve avere le seguenti caratteristiche per essere efficace:

- **Divisibilità**: Deve poter essere divisa in unità più piccole per facilitare le transazioni.
- **Fungibilità**: Deve essere intercambiabile con altre unità della stessa moneta.
- **Stabilità**: Il suo valore deve essere relativamente stabile nel tempo.

Un'unità di conto è una misura standard del valore utilizzata per valutare beni e servizi, nonché un sistema di scala comune per calcolare e confrontare il valore dei prodotti. Le nazioni hanno le proprie unità di conto, come l'euro o la sterlina britannica, ma a livello internazionale il dollaro statunitense è comunemente usato. L'unità di conto è fondamentale per confrontare prezzi, calcolare profitti e perdite, e misurare l'economia di un Paese.

Le proprietà essenziali di un'unità di conto includono divisibilità e fungibilità. Tuttavia, l'inflazione può comprometterne l'affidabilità. Un'unità di conto ideale sarebbe misurabile, stabile e costante come il sistema metrico, ma ciò è difficile da raggiungere dato il valore soggettivo e mutevole.

Bitcoin potrebbe essere una potenziale unità di conto globale in quanto ha un'offerta predefinita e non è soggetto all'inflazione delle valute tradizionali.

Se il Bitcoin diventasse una valuta di riserva globale, potrebbe promuovere il commercio internazionale e la stabilità economica, rendendo più agevoli le transazioni transfrontaliere e riducendo le fluttuazioni valutarie. In generale, un'unità di conto immutata dall'inflazione potrebbe contribuire a una base stabile per l'economia globale, facilitando la pianificazione finanziaria e decisioni economiche più responsabili.

unlocking script

Livello: avanzato

Argomento: tecnologia

Un unlocking script o script di sblocco è uno script che "risolve", o soddisfa, le condizioni impostate su un output da un locking script e consente di spendere l'output.

Gli script di sblocco fanno parte di ogni input di transazione. Nella maggior parte dei casi contengono una firma digitale prodotta dal wallet dell'utente a partire dalla sua chiave privata.

Storicamente, l'unlocking script viene chiamato scriptSig, perché di solito conteneva una firma digitale.

Nella maggior parte delle applicazioni bitcoin, il codice sorgente fa riferimento allo script di sblocco come scriptSig.

Lo script di sblocco viene anche chiamato witness (vedi segwit).

Il termine unlocking script potrebbe essere più adatto perché aiuta a comprendere la gamma molto più ampia di possibilità di questa tecnologia di scripting, perché non tutti gli script di sblocco devono contenere firme.

Un unlocking script è uno script che "risolve", o soddisfa, le condizioni poste su un output da un locking script e consente di spendere l'output. Gli script di sblocco fanno parte di ogni input di transazione. Nella maggior parte dei casi contengono una firma digitale prodotta dal portafoglio dell'utente a partire dalla sua chiave privata.

Ogni nodo di convalida bitcoin convalida le transazioni eseguendo insieme gli script di blocco e di sblocco. Ogni input contiene uno script di sblocco e fa riferimento a un UTXO precedentemente esistente. Il software di convalida copia lo script di sblocco, recupera l'UTXO a cui fa riferimento l'input e copia lo script di blocco da tale UTXO. Lo script di sblocco e quello di chiusura vengono quindi eseguiti in sequenza. L'ingresso è valido se lo script di sblocco soddisfa le condizioni dello script di chiusura (vedere Esecuzione separata degli script di sblocco e di chiusura). Tutti gli input vengono convalidati indipendentemente, come parte della convalida complessiva della transazione.

URSF

Acronimo di: User Rejected Soft Forks

Livello: avanzato

Argomento: tecnologia

URSF sta sia per User Rejected Soft Forks (soft fork rifiutato dagli utenti), che User Resisted Soft Forks (soft fork al quale gli utenti resistono).

Gli URSF sono meglio considerati come l'equivalente speculare degli UASF (User Activated Soft Forks) con segnalazione obbligatoria.
Mentre gli UASF rifiutano i blocchi che non segnalano la disponibilità per un soft fork verso la fine di una finestra di attivazione del soft fork, gli URSF rifiutano i blocchi che invece segnalano.
Se entrambi i client UASF e URSF sono implementati, teoricamente creerebbero una chain split.

UTC

Tempo universale coordinato

Livello: intermedio

Argomento: tecnologia

È lo standard temporale principale in base al quale il mondo regola gli orologi e in particolare gli orologi dei computer, in modo da avere un riferimento univoco indipendentemente dal fuso orario o dall'eventuale applicazione dell'ora legale.

UTF-8

Livello: avanzato

Argomento: tecnologia

UTF-8 (Unicode Transformation Format, 8 bit) è una codifica di caratteri Unicode in sequenze di lunghezza variabile di byte.

UTF-8 usa da 1 a 4 byte per rappresentare un carattere Unicode. Per esempio un solo byte è necessario per rappresentare i 128 caratteri dell'alfabeto ASCII, corrispondenti alle posizioni Unicode da U+0000 a U+007F.

L'uso di Unicode garantisce che le frasi mnemoniche possano includere caratteri di lingue diverse e che le passphrase personalizzate siano rappresentate in modo standardizzato. Tuttavia, per evitare ambiguità nella codifica, è essenziale normalizzare i caratteri Unicode in una forma standard, che garantisca consistenza tra piattaforme e sistemi.

Varianti di normalizzazione Unicode: NFKD e NFC Le varianti di normalizzazione Unicode determinano come i caratteri composti e decomposizioni siano rappresentati in modo coerente. Queste forme sono critiche per applicazioni come la generazione di passphrase Bitcoin, dove anche la minima differenza nella rappresentazione può compromettere l'accesso ai fondi crittografici.

NFC (Normalization Form C) Questa è la forma utilizzata da (BIP 38)[bip-38-passphrase-protected-private-key.html].
Questa forma combina caratteri che possono essere rappresentati sia come carattere base più segni diacritici separati, sia come carattere unico precomposto. Ad esempio, la lettera "é" (U+00E9) in NFC è rappresentata come un unico carattere precomposto.

NFKD (Normalization Form KD) Questa è la forma utilizzata da BIP-39.
In questa forma, i caratteri sono decomposti in caratteri base e segni diacritici separati. Ad esempio, "é" viene scomposto in "e" (U+0065) più il segno diacritico acuto (U+0301). Inoltre, NFKD considera anche l'equivalenza di

compatibilità, trasformando simboli o legature in rappresentazioni canoniche equivalenti.

Utility token

Livello: intermedio

Argomento: legale

Un Utility Token è un token che fornisce delle funzionalità, quali ad esempio l'accesso esclusivo a un prodotto o servizio di una piattaforma. Conferiscono ai titolari diritti di accesso a un servizio o un bene. I titolari di Utility token hanno diritto ad un servizio o ad un bene specifico offerto dal progetto o dall'organizzazione che ha emesso i token. Ad esempio, gli Utility token possono essere utilizzati per acquistare servizi o beni offerti da una piattaforma, come biglietti per un evento o spazio di archiviazione su una rete di computer decentralizzata.

Il MiCA definisce gli Utility Token come un tipo di cripto-asset che è destinato a fornire accesso digitale a un bene o servizio, disponibile su DLT, ed è accettato solo dall'emittente di quel token.

UTXO

Acronimo di: Unspent transaction output

Output non spesi delle transazioni

Livello: intermedio

Argomento: tecnologia

Gli UTXO, o output non spesi delle transazioni, sono spesso indicati semplicemente come *output*.

Per capire gli UTXO possiamo pensare ad un portafoglio che contiene monete e banconote. Ognuno di questi pezzi di valuta metallici o di carta, ha un suo valore, e il valore in un portafoglio corrisponde alla somma dei valori di questi pezzi. Un UTXO è un pezzo discreto di bitcoin, ogni UTXO ha un importo a lui associato. Il saldo di un wallet Bitcoin è dato dalla somma degli importi dei singoli UTXO. Ogni UTXO oltre l'importo ha anche uno script, chiamato scriptPubKey, che specifica come l'UTXO può essere speso o meglio come l'importo può essere sbloccato per essere trasferito ad un nuovo UTXO.

Bitcoin non usa conti e bilanci, i wallet quindi non hanno un importo totale in blockchain, ma un insieme di UTXO ognuno con un suo importo.

Possedere Bitcoin significa essere capace di spendere l'importo degli UTXO, e quindi significa poter eseguire lo script di sblocco degli UTXO.

Una transazione Bitcoin ha un certo numero di UTXO in ingresso, che vengono completamente spesi, creando dei nuovi UTXO in uscita. Quando uno o più UTXO vengono spesi in una transazione, vengono distrutti e vengono creati uno o più nuovi UTXO. Tutti i nodi mantengono un insieme di UTXO esistenti, chiamato UTXO set, che aggiornano ogni volta che un blocco di transazioni crea e distrugge gli UTXO. Questo permette ai nodi di verificare in modo indipendente se una data transazione e il bitcoin che sta tentando di spendere sono validi.

Gli UTXO sono analoghi ai contanti fisici in quanto di solito richiedono il cambio quando vengono spesi. Se Alice possiede un UTXO del valore di 1 BTC e desidera pagare Bob 0,4 BTC, deve spendere l'intero 1 BTC come input. Per inviare a Bob esattamente 0,4 BTC, Alice crea due output: il primo a Bob, dell'importo di 0,4 BTC, e il secondo a se stessa, dell'importo di 0,59 BTC, assumendo che abbia pagato una fee di transazione di 0,01 BTC. Questa transazione consumerà un UTXO e ne creerà 2 nuovi. Si noti che la fee pagata non è di per sé un output, ma è il resto implicito nella somma degli input (1 BTC) meno la somma degli output: 0,4 + 0,59 = 0,99 BTC. Il miner di questa transazione calcola questa fee e la rivendica per se stesso nella transazione coinbase.

Nel modello UTXO, gli input totali devono essere uguali o superiori agli output totali. Questo è uno dei controlli preliminari che i nodi validatori eseguono per verificare se una transazione è valida. Il modello UTXO funziona benissimo in un sistema decentralizzato perché può verificare la presenza di doppie spese in un modo computazionalmente semplice.

Gli UTXO sono costituiti da due parti: l'importo trasferito all'output e lo script di blocco (scriptPubKey) che specifica le condizioni da soddisfare per spendere l'output.

Questi due dati dell'UTXO significano: ci sono tot satoshi in questo UTXO, e potranno essere spesi (trasferiti) da chi riesce a "risolvere" lo script. Lo script, e il modo per essere risolto, può essere di diversi tipi. Il primo, il più semplice, ma ormai obsoleto, è P2PK, Pay-to-Public-Key, paga alla chiave pubblica che è inserita in chiaro nello script. Per risolvere lo script, e quindi poter trasferire i satoshi di quell'UTXO, è sufficiente firmare con la chiave privata corrispondente alla chiave pubblica. Questo primo script è stato presto sostituito da P2PKH, Pay-to-Public-Key-Hash, che sostituisce la chiave pubblica in chiaro con l'hash della chiave pubblica, aggiungendo sicurezza e privacy. A questi primi tipi di script se ne sono aggiunti altri nel tempo: P2PSH, P2WPKH e P2WSH (SegWit), P2TR Pay-to-Taproot per citarne alcuni

UTXO Set

Insieme degli UTXO

Livello: intermedio

Argomento: tecnologia

L'UTXO Set (o UTXO pool) è l'insieme completo di tutti gli UTXO esistenti in un dato momento. Questo set di UTXO viene mantenuto dai full-node in un database in memoria.
La somma delle quantità di ogni UTXO in questo insieme è la supply, o disponibilità totale di bitcoin esistenti in quel momento.
Attraverso l'UTXO Set chiunque può verificare l'offerta totale in qualsiasi momento in modo affidabile. Tutti i nodi mantengono copie identiche dell'insieme UTXO. Quando viene creato un nuovo blocco, il set UTXO viene aggiornato in quanto alcuni UTXO sono stati spesi e ne sono stati creati di nuovi.

L'UTXO Set è importante anche perché permette a tutti i nodi della rete Bitcoin di rilevare e rifiutare i tentativi di doppia spesa, quando qualcuno cerca di spendere lo stesso bitcoin due volte. I nodi devono memorizzare l'intero UTXO in ogni momento per determinare quali bitcoin esistono, e quindi possono essere spesi, in qualsiasi momento.

UVP

Acronimo di: Unique value proposition

Livello: intermedio

Argomento: economia

La proposizione unica di valore è una frase che racchiude in sé la proposta di valore e i tratti unici della tua startup o azienda. È ciò che ti contraddistingue dai numerosi competitor diretti e indiretti ed è ciò che viene in mente ai clienti-investitori quando pensano al brand. È il cuore di tutta la comunicazione di marketing e viene messa in home page del sito e/o in landing page di vendita di ogni prodotto o servizio. È una definizione chiara e inequivocabile dei benefici che il tuo prodotto o servizio offre, dei problemi che risolve ai tuoi clienti e soprattutto di ciò che ti distingue dai competitor.

Validator

Validatore

Livello: intermedio

Argomento: tecnologia

Validatore è un partecipante a una blockchain Proof-of-Stake, coinvolto nella creazione e convalida dei nuovi blocchi da aggiungere alla blockchain, attività che effettua per ottenere il reward.

Nella Proof of Stake di Ethereum 2.0, un validatore mette in stake 32 ETH per partecipare al mantenimento della rete. Se un validatore viene scelto per attestare il blocco successivo, viene ricompensato in ETH come percentuale del

suo stake. Al contrario, i validatori che non svolgono il loro compito, ad esempio se sono offline, ricevono delle penalità, o slash, sotto forma di piccole quantità di ETH sottratte dai loro stake.

Vanity Address

Livello: intermedio

Argomento: tecnologia

Indirizzo pubblico di una criptovaluta creato in modo che alcune lettere e numeri siano personalizzati, solitamente scelti dal proprietario.

VASP

Acronimo di: Virtual Asset Service Provider

Prestatori di servizi in materia di virtual asset

Livello: intermedio

Argomento: politica

Il termine VASP viene utilizzato particolarmente in ambito normativo, ad esempio dal FATF o GAFI, per indicare la categoria di società che forniscono servizi di criptovaluta o virtual asset.
La definizione di VASP include diverse categorie di società, come ad esempio gli exchange di criptovaluta, le piattaforme di trading di criptovaluta, le banche digitali e gli investitori istituzionali.

Il FATF definisce i VASP quali fornitori dei seguenti servizi:

- scambio tra virtual asset e valute fiat;
- scambio tra una o più forme di virtual asset;
- trasferimento di virtual asset;
- custodia e/o amministrazione di virtual asset o strumenti che consentono il controllo di virtual asset;
- partecipazione e fornitura di servizi finanziari relativi all'offerta e/o alla vendita di virtual asset da parte di un emittente.

Il termine VASP viene usato spesso come sinonimo di CASP, anche se la definizione che il MiCA da di CASP è più ampia e include delle fattispecie che non rientrano nella definizione di VASP fatta dal FAFT/GAFI.

In Italia, è stato attivato a maggio 2022 un registro speciale chiamato "Registro dei Prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale", abbreviato come VASP. Questo registro è gestito dall'OAM, l'Organismo per la gestione degli Elenchi degli Agenti in attività finanziaria e dei Mediatori creditizi.

I VASP sono obbligati ad iscriversi in questo registro, e devono continuamente raccogliere e trasmettere informazioni sulle operazioni finanziarie effettuate dai loro clienti.

Il primo report pubblicato a luglio 2023 analizza per la prima volta i dati inviati dai VASP riguardanti il trimestre gennaio-marzo 2023. Questa analisi fornisce una visione dettagliata del mercato delle valute virtuali in Italia e sarà aggiornata periodicamente man mano che gli operatori invieranno ulteriori comunicazioni.

Il report offre anche informazioni sul numero e il tipo di soggetti iscritti al registro dei VASP, includendo uno sguardo su ciò che accade in altri Paesi europei riguardo a questa materia.

vault

Livello: avanzato

Argomento: tecnologia

I Vault sono un tipo di Covenant che richiede che due transazioni separate appaiano in due blocchi diversi affinché un utente possa spendere denaro dal proprio wallet. La prima transazione segnala che qualcuno sta tentando di spendere il denaro e offre all'utente la possibilità di bloccare la seconda transazione che completa la spesa.

Un protocollo vault specifica una quantità minima di tempo o un numero di blocchi che devono passare tra le due transazioni, dando all'utente quel periodo di tempo per notare se qualcuno ha rubato la sua chiave privata e sta tentando di rubare i suoi soldi. Se l'utente rileva il tentativo di furto, la maggior parte dei progetti di vault consente inoltre all'utente di inviare il denaro a un indirizzo sicuro che utilizza uno script più sicuro o di distruggere definitivamente il modo per impedire al ladro di trarre profitto dal proprio attacco.

Alcuni progetti di vault si basano su covenant che richiedono modifiche di consenso a Bitcoin. Altri progetti di vault utilizzano funzionalità di protocollo esistenti oltre a tecniche come la firma delle transazioni molto prima di averne bisogno e quindi la distruzione dei modi per firmare transazioni alternative (eliminando in modo sicuro la chiave di firma o utilizzando multisig per garantire che più chiavi indipendenti debbano essere compromesse).

vByte

Livello: avanzato

Argomento: tecnologia

Prima di SegWit, la dimensione massima di un blocco bitcoin era 1 Megabyte. Con l'introduzione di SegWit, la dimensione massima di un blocco bitcoin è diventata 1 vMegabyte, o 1 milione di vByte.

Il vByte è un'unità di misura del peso dei blocchi e delle transazioni, che si è resa necessaria con l'aggiornamento SegWit, introdotto a partire da Bitcoin Core 0.13.0 rilasciato ad agosto 2016.

La dimensione massima di un blocco può anche essere espressa in Weight Unit, ogni Weight Unit rappresenta 1/4.000.000 della dimensione massima di un blocco.

Un vByte equivale a 4 Weight Unit, o unità di peso, e quindi un blocco è limitato a 1 vMegabyte, ovvero 4 milioni di Weight Unit.

In una transazione legacy, un singolo byte equivale a quattro Weight Unit. Tuttavia, per le transazioni SegWit, ogni byte del Witness, che di solito include le firme, viene conteggiato come una Weight Unit. Pertanto, se un blocco è costituito esclusivamente da transazioni legacy, il limite di dimensione del blocco di 4 milioni di Weight Unit equivale ancora a 1MB, ma se nel blocco sono incluse transazioni SegWit, il limite di dimensione del blocco consente fino a 4MB di dati; questo fa in modo che non sia più possibile usare il byte per calcolare agevolmente dimensione di transazioni e blocchi, e quindi viene utilizzato il vByte.

I wallet di solito calcolano e visualizzano le tariffe delle fee in termini di sats/vByte, ovvero la tariffa viene pagata per vByte di dati utilizzati. Pertanto, più grande è la transazione, maggiore deve essere la fee totale per garantire la velocità di verifica desiderata. Questa impostazione rende anche le transazioni SegWit più economiche di quelle normali, poiché un byte di Witness data equivale solo a 1 Weight Unit (1/4 di vByte), mentre un byte di dati non-Witness equivale a 4 Weight Unit (1 vByte).

version

versione

Livello: intermedio

Argomento: tecnologia

Il campo version, version number o nVersion, è un campo presente come componente nel block header e nelle transazioni, con diversi scopi.

È un numero di 4 byte (32 bit). Il formato utilizzato per la sua rappresentazion è di tipo little-endian, ovvero inizia dal byte meno significativo (estremità più piccola) per finire col più significativo.

Il valore 01000000 rappresenta version = 1.

Blocchi Nel contesto dei blocchi, nVersion viene utilizzato per segnalare la versione del formato di un blocco. Svolge un ruolo cruciale nell'attivazione dei soft fork, in cui specifici bit all'interno del campo nVersion vengono usati per indicare il supporto dei miner agli aggiornamenti del protocollo. Ad esempio,

BIP9 descrive un meccanismo in cui singoli bit del campo nVersion vengono impiegati per segnalare la disponibilità a nuove funzionalità o regole, permettendo un approccio più granulare nell'implementazione dei soft fork.

Transazioni All'interno delle transazioni, nVersion indica la versione del formato della transazione in uso. Questo consente di apportare modifiche retrocompatibili alla struttura delle transazioni senza interrompere il funzionamento della rete esistente.

Nelle transazioni Bitcoinche indica la versione del formato della transazione. Questa versione può cambiare nel tempo per introdurre nuove funzionalità o modifiche al protocollo Bitcoin.

Valori attualmente utilizzati sono:

- 1 (Introdotto dalla prima versione di Bitcoin) → Supporto per transazioni di base.
- 2 (BIP 68, 2016) → Introduzione del Relative Locktime per migliorare i canali di pagamento. È stato usato per segnalare la disponibilità di transazioni SegWit.
- Version 1: È la versione originale e più comune delle transazioni Bitcoin, introdotta fin dall'inizio del protocollo.
- Version 2: Introdotta con BIP68, BIP112 e BIP113, abilita nuove funzionalità come:
  - Lock-time relativo (usando nSequence)
  - Verifica della firma con CHECKSEQUENCEVERIFY
  - Support per il consenso basato sul tempo mediano dei blocchi

Coordinamento: nVersion può anche essere impiegato per coordinare varie funzionalità, come l'interpretazione di altri campi, ad esempio nSequence nel contesto dei relative time locks. È in corso un dibattito su come i bit di nVersion e nSequence vengano valorizzati e gestiti, considerando sia l'ottimizzazione dello spazio che l'estensione delle capacità.

Virgin Bitcoin

Livello: intermedio

Argomento: tecnologia

Un bitcoin che non è mai stato speso. Sono monete che non hanno una cronologia delle transazioni, poiché è stato assegnato al miner che ha minato il blocco ma non ha mai lasciato il suo wallet

Virtual asset

Livello: intermedio

Argomento: politica

Il termine virtual asset è spesso usato in ambito normativo per indicare le criptovalute. Il FATF definisce il virtual asset come una rappresentazione digitale di valore che può essere scambiata digitalmente, o trasferita, e può essere utilizzata per il pagamento o l'investimento. I virtual asset non includono rappresentazioni digitali di valute fiat, security e altri asset finanziari che sono già coperti altrove nelle raccomandazioni del FATF.

VM

Acronimo di: Virtual Machine

macchina virtuale

Livello: avanzato

Argomento: tecnologia

Una virtual machine (VM), in italiano "macchina virtuale", è un software che emula un ambiente informatico completo all'interno di un sistema operativo o di un altro ambiente informatico. In altre parole, una VM è un'istanza virtuale di un computer che esiste all'interno di un computer fisico. Questa tecnologia consente di eseguire più sistemi operativi o ambienti software separati su una singola macchina fisica.

Nell'ambito delle criptovalute, una "virtual machine" si riferisce principalmente a una funzionalità che consente di eseguire dei particolari programmi chiamati smart contract in un contesto decentralizzato basato sulla block chain.

Il caso più noto è la Ethereum Virtual Machine implementata su Ethereum.

Volatility

Volatilità

Livello: base

Argomento: finanza

In finanza, la volatilità descrive quanto velocemente e di quanto cambia il prezzo di un asset. Poiché è una misura della rapidità e del grado di variazione dei prezzi, la volatilità viene spesso utilizzata come misura del rischio di investimento.

Bitcoin come forma di denaro digitale è stato criticato per essere troppo volatile per essere un store of value.
La sua volatilità significa che il prezzo di Bitcoin cambia molto rapidamente e può essere imprevedibile.
Questo è principalmente dovuto al fatto che l'offerta di Bitcoin è fissa e non

può essere facilmente adattata alle variazioni della domanda, rendendolo più suscettibile alle fluttuazioni di prezzo.

Tuttavia, ci sono previsioni che questa instabilità diminuirà con il tempo. Quando più persone iniziano ad utilizzare Bitcoin e quando ci sono più prodotti finanziari legati a Bitcoin disponibili per gli investitori, la volatilità potrebbe ridursi. La storia mostra che nuovi beni, come l'oro, hanno avuto volatilità simile prima di diventare stabili come store of value.

Al momento, Bitcoin è considerato un nuovo tipo di risorsa che sta diventando sempre più accettato e sta attraversando un processo di finanziarizzazione, cioè diventando un oggetto di investimento più tradizionale. Ma in confronto ad altri beni come l'oro, è detenuto da un numero di persone più limitato.

Si prevede che, con un aumento di investimenti e strumenti finanziari legati a Bitcoin, la volatilità potrebbe diminuire gradualmente nel tempo. Una maggiore diffusione di Bitcoin potrebbe aiutare a stabilizzare il suo prezzo in quanto i nuovi partecipanti avranno meno impatto sul mercato.

Tuttavia, nonostante la possibilità che la volatilità diminuisca rispetto ai livelli attuali, resta comunque più alta rispetto ad altri tipi di investimenti finanziari.

Questa volatilità di Bitcoin è simile a quella che ha caratterizzato l'oro quando era anch'esso in una fase di incertezza nelle prime fasi di investimento. Anche se può sembrare rischioso, alcuni investitori considerano questa volatilità come un'opportunità, come è successo con l'oro, che ha visto un aumento considerevole del valore nel corso del tempo.

Infine, la volatilità di Bitcoin è anche legata al fatto che il suo mercato è resistente agli interventi esterni. Nessuna banca centrale o governo può influenzarne artificialmente la sua emissione. Questo potrebbe essere preferibile rispetto a un controllo artificiale del prezzo che potrebbe portare a instabilità nel lungo termine.

In sostanza, la volatilità di Bitcoin è dovuta alla sua offerta fissa e al suo mercato libero da manipolazioni esterne. Sebbene possa sembrare instabile, alcuni lo vedono come un aspetto positivo rispetto a un controllo artificiale che potrebbe portare a problemi più grandi nel futuro.

Volume

Livello: base

Argomento: finanza

La quantità di criptovaluta che è stata scambiata durante un certo periodo di tempo, ad esempio le ultime 24 ore o più. Il volume può mostrare la direzione e il movimento della criptovaluta, nonché una previsione del prezzo futuro e della sua domanda.

Voting power

Livello: intermedio

Argomento: politica

All'interno di alcune blockchain gli utenti hanno la possibilità di votare il modo in cui la chain dovrebbe cambiare il suo comportamento mentre è in esecuzione. In queste catene, il potere di voto rappresenta il peso che il voto di un utente (o validatore) avrà in tale scenario. Un potere di voto più alto implicherà una maggiore capacità di influenzare il risultato della votazione stessa.

vsize

Acronimo di: Virtual size

Livello: avanzato

Argomento: tecnologia

vsize, o Virtual size, che utilizza come unità di misura i vbytes o virtual byte, è una misura utilizzata per confrontare le dimensioni di diverse transazioni Bitcoin tra loro in proporzione al limite massimo di dimensione del blocco, ed è una modalità alternativa alle Weight unit. Un vbyte è pari a 4 Weight unit. Ciò significa che la dimensione massima del blocco misurata in vsize è di 1 milione di vbyte.

WAGMI

Acronimo di: We're All Gonna Make It

Ce la faremo

Livello: avanzato

Argomento: politica

A volte usata anche nella forma WGMI, è una espressione usata nel contesto delle criptovalue e in particolare nelle comunità NFT, su Twitter e nei gruppi Discord relativi agli NFT. Può essere tradotta come "ci arriveremo tutti" oppure "ce la faremo tutti". WAGMI è spesso espresso in reazione a buone notizie o dopo aver intrapreso azioni che generalmente si ritiene portino a risultati positivi.

È l'opposto di NGMI.

Wallet

Portafoglio

Livello: base

Argomento: tecnologia

I wallet Bitcoin sono strumenti fondamentali per interagire con l'ecosistema Bitcoin. Servono per conservare, inviare e ricevere Bitcoin, ma non memorizzano fisicamente i Bitcoin stessi, i quali esistono esclusivamente sulla blockchain.

Come funzionano i wallet Bitcoin

Il termine "wallet" può essere fuorviante, poiché i Bitcoin non sono conservati all'interno del wallet. Piuttosto, il wallet gestisce le chiavi crittografiche che consentono l'accesso ai Bitcoin registrati sulla blockchain. In pratica, i wallet possono essere considerati come un portachiavi che memorizza coppie di chiavi private e pubbliche.

Quando un utente invia Bitcoin, firma la transazione con la propria chiave privata. La transazione viene quindi trasmessa alla rete, verificata e registrata nella blockchain pubblica.

Tipologie di wallet

I wallet Bitcoin possono essere classificati in base a diverse caratteristiche:

Formato fisico o digitale:

- **Software wallet**: Applicazioni installabili su computer o dispositivi mobili.
- **Hardware wallet**: Dispositivi fisici progettati per la sicurezza delle chiavi private.

Connessione a Internet:

- **Hot wallet**: Connessi a Internet, offrono maggiore comodità ma sono più vulnerabili agli attacchi.
- **Cold wallet**: Non connessi a Internet, garantiscono una sicurezza superiore.

***Custodia delle chiavi*:**

- **Custodial wallet**: Le chiavi private sono gestite da un servizio terzo fiduciario. In questo caso, l'utente non ha il pieno controllo dei propri fondi.
- **Non-custodial wallet**: Le chiavi private sono interamente sotto il controllo dell'utente.

Secondo il regolamento europeo MiCA , i custodial wallet sono definiti come Hosted Wallet, mentre i non-custodial wallet sono indicati come Unhosted Wallet.

Altri tipi di wallet Nel tempo sono emerse diverse varianti di wallet Bitcoin, tra cui:

- **Paper wallet**: Stampano le chiavi su carta.
- **Brain wallet**: Memorizzano le chiavi nella memoria dell'utente.
- **Multisig wallet**: Richiedono più firme per autorizzare una transazione.
- **Watch-only wallet**: Consentono di monitorare i saldi senza avere accesso alle chiavi private.
- **Lightning wallet**: Utilizzati per transazioni rapide su reti di secondo livello.

Funzionalità dei wallet Bitcoin Un wallet Bitcoin svolge diverse funzioni:

- **Generazione e gestione delle chiavi**: Il wallet genera chiavi private e pubbliche o consente di importare chiavi esistenti.
- **Firma delle transazioni**: Le chiavi private vengono utilizzate per autorizzare i trasferimenti di Bitcoin.
- **Interfaccia utente**: I wallet forniscono un'interfaccia intuitiva per gestire saldi, visualizzare cronologie delle transazioni e generare indirizzi per ricevere pagamenti.
- **Interazione con la blockchain**: Il wallet comunica con nodi Bitcoin per inviare e ricevere transazioni.

In sintesi, i wallet Bitcoin semplificano la gestione della complessità tecnica di Bitcoin, rendendo possibile per gli utenti conservare e utilizzare i propri Bitcoin in modo sicuro ed efficace.

Wash Trading

Livello: intermedio

Argomento: legale

Il wash trading è un'operazione di manipolazione del mercato che avviene attraverso acquisti e vendite volte a far apparire un titolo, una criptovaluta o un token più interessante poiché sembra avere molti movimenti e un prezzo in crescita. Questo è fatto per manipolare il prezzo o per mostrare un volume di scambi sostanzialmente aumentato rispetto all'importo effettivamente negoziato senza questa manipolazione. In alcuni casi, il wash trading viene eseguito da investitori che agiscono sia come compratori che come venditori del titolo, mentre in altre situazioni coinvolge un trader e un broker che sono collusi tra loro.

Il wash trading è proibito nei titoli convenzionali e nei futures, ma il wash trading che coinvolge gli NFT non è ancora stato oggetto di azioni legali. Storicamente, il wash trading è stato motivo di preoccupazione per gli scambi di criptovalute che cercano di far apparire i loro volumi di scambio più grandi di quanto siano in realtà.

Nel caso del wash trading di NFT, l'obiettivo è far apparire il proprio NFT più prezioso di quanto sia in realtà "vendendolo" a un nuovo portafoglio controllato dal proprietario originale. Questo è relativamente facile con gli NFT, dato che molte piattaforme di trading NFT permettono agli utenti di commerciare collegando il loro portafoglio alla piattaforma senza bisogno di identificarsi.

Attraverso l'analisi della blockchain, è possibile tracciare il wash trading di NFT osservando le vendite di NFT a indirizzi che sono stati autofinanziati, ovvero finanziati dall'indirizzo di vendita o dall'indirizzo che inizialmente ha finanziato l'indirizzo di vendita. Questa analisi ha mostrato come alcuni venditori di NFT abbiano effettuato numerose operazioni di wash trading.

Watchtower

Livello: avanzato

Argomento: tecnologia

Le Watchtower (letteralmente torri di controllo) sono un servizio di sicurezza della rete Lightning che monitorano i canali di pagamento alla ricerca di potenziali violazioni del protocollo. Se uno dei partner del canale va offline o perde il proprio backup, una Watchtower conserva i backup e può ripristinare le informazioni del canale.

Le Watchtower monitorano anche la blockchain Bitcoin e possono inviare una penalty transaction se uno dei partner cerca di "barare" trasmettendo uno stato non aggiornato. Le Watchtower possono essere gestite dagli stessi partner del canale o come servizio a pagamento offerto da terzi. Le Watchtower non hanno alcun controllo sui fondi dei canali stessi.

Le Watchtower registrano lo stato della rete Lightning visibile pubblicamente in ogni momento. Le Watchtower sono progettate per memorizzare i dati che vengono utilizzati nelle justice transaction per dimostrare che qualcuno ha mentito o ha firmato una richiesta di chiusura del canale fraudolenta.

Il servizio fornito da watchtowers consente ai client di andare offline per un periodo di tempo significativo senza doversi preoccupare che i loro fondi vengano rubati da una controparte. Alle watchtower non viene affidato alcun fondo, ma solo la responsabilità di monitorare la blockchain e di trasmettere le transazioni, anche se le remedy transaction alla violazione possono essere progettate in modo che la watchtower riceva una parte dei fondi salvaguardati se i suoi servizi sono necessari.

Le Watchtower sono un meccanismo per esternalizzare il monitoraggio e la risoluzione delle penalità delle violazioni del protocollo Lightning.

Il protocollo Lightning mantiene la sicurezza attraverso un meccanismo di penalità. Se uno dei vostri partner di canale trasmette una vecchia commitment transaction, il vostro nodo dovrà esercitare la clausola di revoca e trasmettere una penalty transaction per evitare di perdere i propri fondi. Ma se il vostro nodo non funziona durante la violazione del protocollo, potreste perdere i vostri fondi.

Per risolvere questo problema, possiamo utilizzare una o più Watchtower per esternalizzare il lavoro di monitoraggio delle violazioni del protocollo e di emissione delle penalty transaction. La configurazione di una watchtower è composta da due parti: un server watchtower (o semplicemente watchtower) che monitora la blockchain e un client watchtower che chiede al server watchtower questo servizio di monitoraggio.

Le Watchtower inviano remedy transaction, transazioni per rimediare alla violazioni LN (justice transaction) quando rilevano che una delle controparti dei suoi clienti ha trasmesso una transazione di chiusura del canale non aggiornata.

Attualmente, tali watchtower sono implementate solo come watchtower altruistiche. Ciò significa che le watchtower non vengono compensate per l'intervento riuscito in caso di violazione del canale. Invece, funzionano senza compensazione o addebitano il costo del loro servizio senza garanzia di successo.
Come tale, un operatore di nodo che desidera utilizzare una watchtower di solito esegue questa watchtower da solo, idealmente su una macchina, una rete e una geolocalizzazione separate dal nodo che sta proteggendo. Un nodo può utilizzare più watchtower e una watchtower può proteggere più nodi.

Web3

Livello: avanzato

Argomento: tecnologia

Web3 è una evoluzione del Web con caratteristiche di decentralizzazione basata su blockchain pubbliche, con la possibilità di eseguire dApps.

L'integrazione tra il web e la blockchain avviene utilizzando un wallet integrato con il browser, tipicamente Metamask.

In questo modo è possibile registrarsi e accedere ai siti senza la necessità di fornire dati personali.

Il termine Web3 è spesso usato come scorciatoia per discutere della nuova fase di Internet. Descrive l'abbandono dell'era dei social media centralizzati e delle massicce piattaforme di e-commerce e l'arrivo a un web nel quale i dati controllati dall'utente. Web3, in senso colloquiale, è semplicemente un termine usato per fini di marketing per indicare qualsiasi cosa ha a che fare con le cripto.

Il nome nasce da Web3.js, una libreria JavaScript che consente di interagire con un nodo Ethereum locale o remoto utilizzando HTTP, IPC o WebSocket. In altre parole, consente agli sviluppatori di creare applicazioni web che possono interagire con la blockchain Ethereum.

Web3.js fornisce una serie di API che consentono agli sviluppatori di eseguire operazioni come:

- Connettersi a un nodo Ethereum
- Inviare e ricevere transazioni
- Creare e gestire contratti intelligenti
- Interagire con altri dApp (applicazioni decentralizzate) sulla blockchain Ethereum

Web3.js è una libreria molto popolare tra gli sviluppatori di applicazioni Ethereum, ed è utilizzata da molti progetti come MetaMask e Truffle.

weight unit

Livello: avanzato

Argomento: tecnologia

Weight unit o unità di peso è l'unità utilizzata per misurare la dimensione delle transazioni e dei blocchi a partire dall'aggiornamento di SegWit. Le weight unit sono abbreviate in **wu**. Prima di SegWit, le transazioni e i blocchi erano misurati in byte e i blocchi erano limitati a 1MB o 1 milione di byte. Dopo l'aggiornamento di SegWit, le transazioni e i blocchi sono misurati in weight unit e i blocchi sono limitati a 4 milioni di weight unit.

In una transazione legacy, un singolo byte equivale a quattro weight unit. Tuttavia, per le transazioni SegWit, ogni byte nel Witness, che di solito include le firme, viene conteggiato come 1 weight unit ciascuno. Questo sconto consente alle transazioni SegWit di pagare fee inferiori rispetto alle transazioni non SegWit.

Pertanto, se un blocco è costituito esclusivamente da transazioni legacy, il limite di dimensione del blocco di 4 milioni di weight unit equivale ancora a 1MB, ma se nel blocco sono incluse transazioni SegWit, il limite di dimensione del blocco consente fino a 4MB di dati.

A seguito dell'aggiornamento SegWit, per avere una unità di misura del peso dei blocchi e delle transazioni è stato introdotto il vByte. Un vByte equivale a 4 Weight unit, e quindi un blocco è limitato a 1 vMegabyte, ovvero 4 milioni di weight unit.

Whale

Balena

Livello: base

Argomento: politica

è usato per descrivere un individuo o un'organizzazione che detiene una grande quantità di una particolare critpovaluta. Non c'è alcuna soglia esatta per questa definizione, per alcuni una balena Bitcoin dovrebbe avere almeno 1000 Bitcoin. Una balena può anche essere definita come una persona che ha abbastanza coin o token per causare un impatto significativo sui prezzi di mercato, acquistando o vendendo grandi quantità, e quindi di fare ad esempio Pump and dump

Whitelist

Livello: intermedio

Argomento: finanza

Whitelist può assumere diversi significati nel mondo delle criptovalute.

In generale una whitelist è una lista di elementi (email, account, wallet o altri identificativi) che sono stati approvati o autorizzati. Negli eventi di lancio o airdrop, per ICO e NFT, possono esserci un insieme di utenti privilegiati che possono partecipare inizialmente e questi vengono inseriti nella relativa whitelist. Gli investitori che vogliono partecipare ad una ICO potrebbero essere inseriti nella whitelist dopo aver fornito le loro informazioni personali, ad esempio per esigenze di KYC.

Le aziende di criptovalute possono anche pagare per essere aggiunte a una whitelist di fornitori di servizi internet.

Per quanto riguarda gli indirizzi withdrawal da servizi quali Exchange, la whitelist si riferisce a una lista di indirizzi di wallet considerati affidabili. In tali casi solo gli indirizzi inseriti nella whitelist possono prelevare fondi dai conti di scambio.

Whitepaper

Livello: intermedio

Argomento: tecnologia

Il whitepaper, traducibile in italiano con Libro bianco anche se spesso viene usato il termine inglese, è un documento informativo solitamente emesso da un soggetto, un'azienda o un'organizzazione per presentare le caratteristiche di una soluzione, prodotto o servizio che ha ideato, offre o intende offrire.

Il 31 Ottobre 2008 Satoshi Nakamoto con un messaggio nella mailing list Cryptography annuncia che sta lavorando ad un nuovo sistema di contanti elettronici

completamente peer-to-peer, senza terze parti fidate e pubblica il whitepaper di Bitcoin, un pdf di 9 pagine dal titolo: "*Bitcoin: A Peer-to-Peer Electronic Cash System*".

I whitepaper dovrebbero essere dei documenti di specifiche tecniche anche se spesso sono scritti come documenti di promozione e marketing per invogliare o persuadere i potenziali clienti a saperne di più o ad acquistare un particolare prodotto, servizio, tecnologia o metodologia. Nel mondo delle criptovalute, i whitepaper sono usati come mezzo per descrivere la struttura, il piano e la concezione di una rete blockchain.

Nel caso di Bitcoin, il white paper è un documento molto importante in termini storici e un documento molto importante in termini di trasmissione dei concetti più basilari alla base della progettazione di Bitcoin come sistema astratto, ma non ha effettivamente definito e conseguentemente creato la rete Bitcoin: la nascita di Bitcoin avviene infatti circa due mesi dopo con il rilascio del programma e del suo codice, e il 3 gennaio 2009 con la creazione del primo blocco della blockchain bitcoin, il Genesis block.

Nel white paper c'è solo una descrizione di alto livello di alcuni concetti, in particolare viene esaminato in modo estremamente semplificato la una soluzione al problema della double spend, ma non esiste un'analisi approfondita del protocollo generale e della struttura della rete, non esiste una definizione completa del protocollo stesso e gran parte del protocollo non è nemmeno menzionato nel documento. Il termine script neanche compare nel white paper, eppure è una componente fondamentale nel modo con cui i bitcoin possono essere spesi, o meglio trasferiti attraverso la creazione di transazioni e script di blocco e sblocco. Anche la proof of work nel white paper non viene descritta in termini di dettagli importanti quali il periodo di difficoltà, il numero di blocchi in media

Alcune cose delle quali parla il white paper Bitcoin non sono mai state nemmeno implementate come descritte, quali ad esempio i client SPV Simplified Payment Verification che dovrebbero ricevere degli avvisi dai nodi della rete quando questi incontrano un blocco non valido.

Satoshi scrisse il codice del programma Bitcoin prima di scrivere il whitepaper. Nelle sue prime e-mail, Satoshi menziona che aveva lavorato sul codice Bitcoin per 2 anni prima di pubblicare il whitepaper: "In realtà ho fatto questo tipo di operazione al contrario. Ho dovuto scrivere tutto il codice prima di potermi convincere."

Parti del whitepaper non sono più rilevanti, nel corso degli anni sono cambiate così tante cose che gli sviluppatori di Bitcoin mantengono una sorta di elenco ufficiale delle incongruenze e imprecisioni nel white paper di Bitcoin.

Craig Steven Wright, che aveva affermato di essere Satoshi Nakamoto e che poi è stato condannato per il fatto di non esserlo, era riuscito nel 2021 con una causa legale a impedire ai residenti del Regno Unito (UK) di accedere al whitepaper presente su alcuni siti quali bitcoin.org

I Whitepaper secondo il MiCA Il regolamento europeo MiCA si riferisce così ai whitepaper:

Quando si effettua un'offerta pubblica di cripto-asset, diversi da ART asset-referenced token o EMT token di moneta elettronica, nell'Unione o quando viene chiesta l'ammissione di cripto-asset alla negoziazione su una piattaforma di negoziazione per tali cripto-asset, gli offerenti o le persone che chiedono l'ammissione alla negoziazione dovrebbero produrre, notificare alla loro autorità competente e pubblicare un documento informativo ("un whitepaper sui cripto-asset") contenente informazioni obbligatorie. Tale whitepaper sui cripto-asset dovrebbe contenere informazioni generali sull'emittente, l'offerente o la persona che chiede l'ammissione alla negoziazione, sul progetto da realizzare con il capitale raccolto, sull'offerta pubblica di cripto-asset o sulla loro ammissione alla negoziazione su una piattaforma di negoziazione per cripto-asset, sui diritti e gli obblighi legati ai cripto-asset, sulla tecnologia sottostante usata per tali attività e sui rischi correlati. Tuttavia, non si prevede che il whitepaper contenga una descrizione di rischi che sono imprevedibili e che è molto improbabile che si concretizzino. Le informazioni contenute nel white paper sugli asset crittografici e nelle comunicazioni di marketing, compresi i messaggi pubblicitari e il materiale di marketing, anche attraverso nuovi canali come i piattaforme di social media, devono essere corrette, chiare e non fuorvianti. I messaggi pubblicitari e il materiale di marketing dovrebbero essere coerenti con le informazioni fornite nel whitepaper sui cripto-asset cripto-asset.

WIF

Acronimo di: Wallet import format

Livello: intermedio

Argomento: tecnologia

Wallet Import Format (WIF) è un formato standard per visualizzare e salvare le chiavi private Bitcoin.

Lo standard WIF è stato creato per consentire a tutti i portafogli Bitcoin di importare ed esportare chiavi private.

Il processo di codifica di una chiave privata in formato WIF è il seguente: le chiavi private sono semplicemente grandi numeri.

Il formato WIF aggiunge un byte di prefisso (0x80 per mainnet e 0xef per testnet) in modo che quasi tutte le chiavi private Bitcoin inizino con "5" o "K" su mainnet. Viene aggiunto un byte "0x01" alla fine della chiave privata se la chiave pubblica corrispondente deve utilizzare il Formato SEC compresso. Infine, alla chiave privata codificata in byte viene aggiunto un checksum SHA-256 doppio di quattro byte, al fine di prevenire errori di battitura o manomissioni. Questa stringa di byte viene quindi convertita da byte a Base58Check.

Il formato WIF è il modo in cui si interagiva con le proprie chiavi private agli albori di Bitcoin. In quel periodo prima dell'arrivo dei Wallet deterministici gerarchici, si poteva generare una chiave privata alla volta.

Withdrawal

Prelievo

Livello: base

Argomento: finanza

Prelievo di una somma di denaro o criptovalute. È il termine che utlizzato sugli exchange per spostare i fondi su un altro conto, ad esempio tramite bonifico sul conto corrente bancario dell'utente o tramite transazione blockchain sul wallet dell'utente.

witness

Livello: avanzato

Argomento: tecnologia

Il Witness, traducibile letteralmente come testimone, all'interno di una transazione è quella parte che rappresenta la firma di sblocco.

La transazione Bitcoin può quindi essere considerata composta da 2 segmenti:

- I dati della firma, chiamati witness
- il Merkle tree record di chi invia o riceve i bitcoin

Prima di Segwit, questi due segmenti erano uniti, mentre con Segwit i due segmenti vengono divisi, rimuovendo il witness dalla porzione originale e aggiungendolo in fondo come struttura separata. La sezione originale continua a trattenere i dati di chi invia o riceve e la nuova struttura witness contiene gli script e le firme. Questo comporta un vantaggio anche in termini di scalabilità ai fini dell'occupazione di un blocco, perché il segmento dati originale viene contato normalmente ma il segmento witness viene contato come un quarto della sua grandezza reale.

Il Witness di una transazione è una sezione delle transazioni SegWit non inclusa quando una transazione viene sottoposta a hash e firma. Il witness contiene gli Script Witness per tutti gli input SegWit di una transazione. Lo Script Witness è analogo a uno ScriptSig nelle transazioni legacy (quelle con il vecchio formato prima di segwit): contiene le firme e gli script necessari per spendere un precedente output SegWit.

Poiché lo ScriptSpend, script di spesa, è incluso nel witness, lo ScriptSig delle transazioni SegWit viene lasciato vuoto. Non essendo il witness incluso nell'hash di una transazione, non influisce sul txid. Questa architettura è stata implementata per eliminare la Transaction Malleability.

I dati del witness sono considerati parte di una transazione e vengono memorizzati insieme a ogni transazione da tutti i nodi Bitcoin che hanno implementato SegWit. Tuttavia, i dati dei witness ricevono uno sconto quando viene calcolato il peso di una transazione. Mentre un normale byte di una transazione equivale a 4 unità di peso, un byte di dati del witness pesa solo 1 unità di peso. Questo sconto rende le uscite SegWit meno costose di quelle legacy. Inoltre, aumenta effettivamente la dimensione massima dei blocchi da 1MB a 4MB.

Per garantire che il witness di una transazione non possa essere alterato una volta inserito nella blockchain, viene calcolato un witness txid, o wtxid, separato. Questo wtxid viene utilizzato per creare un albero di Merkle distinto di tutte le transazioni SegWit in un blocco, simile al normale albero di Merkle di un blocco. Questo albero Merkle viene aggiunto come scriptPubKey di un output coinbase vuoto utilizzando OP_RETURN.

Wrapped SegWit

Livello: avanzato

Argomento: tecnologia

Wrapped SegWit, o P2SH Wrapped SegWit, , indicato anche con il termine Nested SegWit, è un'implementazione inclusa nell'aggiornamento di SegWit pensata per consentire ai wallet e ad altri software Bitcoin di supportare più facilmente SegWit.

Con P2SH Wrapped SegWit i nodi e wallet più vecchi che non supportano ancora SegWit, vedono le transazioni SegWit come transazioni P2SH e anche se non vedono le firme e gli script le considerano valide.

Per porterlo fare, i due script SegWit nativi, P2WPKH e P2WSH, vengono utilizzati come redeemScript di una transazione P2SH, ottenendo rispettivamente i tipi di script SegWit con wrapping di P2SH-P2WPKH e P2SH-P2WSH.

Gli utenti che ricevono bitcoin su indirizzi wrapped SegWit sono comunque in grado di risparmiare sulle commissioni di transazione utilizzando il campo Witness, anche se in misura minore rispetto a quando utilizzano script SegWit nativi.

Come tutti gli indirizzi P2SH, gli indirizzi SegWit incapsulati inizieranno con un 3 e utilizzeranno la codifica Base58, mentre gli indirizzi SegWit nativi inizieranno con bc1 e utilizzeranno la codifica Bech32.

Il wallet di Bitcoin Core consente di essere configurato tramite il parametro *addresstype* con i seguenti valori:

- Legacy
- P2SH Wrapped SegWit (impostato come default)
- Bech32

wtxid

Livello: avanzato

Argomento: tecnologia

Il wtxid, o witness transaction ID, è la versione del txid (o identificativo della transazione) a seguito del soft fork introdotto con SegWit.

Quando viene calcolato un normale txid, esso esclude le informazioni sul witness e quindi se una transazione non ha input SegWit, il suo wtxid è identico al suo txid.

Il wtxid è calcolato prendendo il doppio hash SHA-256 di una transazione serializzata, compresi il marcatore SegWit, la versione e il witness.

I wtxid vengono utilizzati dai miner per costruire un Merkle tree, che viene incluso in un output della transazione coinbase. Questo elimina qualsiasi malleabilità del witness di una transazione una volta che questa è stata inclusa in un blocco.

wumbo channel

Livello: avanzato

Argomento: tecnologia

I wumbo channel sono canali Lightning che hanno la capacità di contenere più fondi e gli utenti possono inviare transazioni in bitcoin di dimensioni maggiori.

Inizialmente le dimensioni dei canali Lightning erano limitati a un massimo di 0,1677 BTC, e dopo diversi anni di sviluppo, nel Lightning Network Specification Meeting del 2018 si è deciso di consentire alle implementazioni di effettuare l'opt-in sui wumbo channel senza limiti di quantità a livello di protocollo, anche se le implementazioni e gli utenti possono ancora rifiutare di accettare canali di dimensioni superiori a quelle personalizzabili.

Nel 2020 è stato annunciato che i vincoli saranno rimossi per consentire ai clienti di avere canali più grandi, e il supporto per questa nuova funzionalità, successivamente denominata `option_support_large_channel`, è stato ampiamente implementato nel software Lightning Network dal 2020.

XBT

Livello: intermedio

Argomento: finanza

La sigla BTC per indicare bitcoin, usata come ticker viola l'ISO 4217 dell'International Organization for Standardization e, in base a questo standard, va contro la valuta del Bhutan.

Secondo la norma ISO 4217, che definisce le regole per le valute nazionali e le loro nomenclature e anche per gli asset non garantiti dal governo come l'oro (XAU) e l'argento (XAG), le prime due lettere del carattere a tre lettere dovrebbero indicare il codice del Paese e l'ultima lettera dovrebbe indicare la lettera iniziale della valuta nazionale.

Dal momento che il codice paese BT sta per il paese Bhutan, BTC è in conflitto con la valuta del Bhutan che è il BTN (Ngultrum bhutanese). Ecco perché a volte su alcuni Exchange, piattaforme di trading o altri siti che visualizzano le quotazioni per Bitcoin viene utilizzato il nome alternativo **XBT** al posto di BTC.

XBT non è comunque ufficializzato dall'ISO 4216.

Xprv

Acronimo di: Extended Private Key

Chiave privata estesa

Livello: intermedio

Argomento: tecnologia

Una chiave privata estesa, o Xprv, è una chiave privata che può essere utilizzata per derivare chiavi private secondarie da un Wallet HD, Gerarchico Deterministico.

Quasi tutti i wallet Bitcoin utilizzano questo formato HD dall'adozione del BIP 32, in quanto consente a un'unica chiave privata estesa, detta master private key, di eseguire il backup e rigenerare tutte le chiavi pubbliche e private di un determinato wallet.

Le chiavi private master e le chiavi private estese vengono spesso confuse. Una chiave privata estesa è una qualsiasi chiave privata che può essere utilizzata per generare chiavi private secondarie. Una chiave privata master è la chiave privata estesa alla radice di un albero HD e deriva direttamente dal seed di un wallet HD.

Se una singola chiave privata viene divulgata, si possono perdere i fondi associati a quella singola chiave. Tuttavia, se la vostra chiave Xprv viene divulgata, tutti i fondi associati a tutte le chiavi private che la compongono sono compromessi.

Tutte le chiavi Xprv iniziano con le lettere "Xprv" seguite da una lunga serie di lettere e numeri.

L'Xpriv è una metà della coppia di chiavi master, l'altra è una Xpub o chiave pubblica estesa.

Xpub

Acronimo di: Extended Public Key

Chiave pubblica estesa

Livello: intermedio

Argomento: tecnologia

Una chiave pubblica estesa, o Xpub, è una chiave pubblica che può essere utilizzata per derivare chiavi pubbliche figlie di un Wallet HD, Gerarchico Deterministico.

Una chiave pubblica estesa è uno standard Bitcoin stabilito da BIP 32 ed è utilizzato principalmente da un wallet per creare delle chiavi pubbliche derivandole da quella principale.

La condivisione della tua Xpub con servizi affidabili consente diversi casi d'uso, tuttavia, non dovrebbe essere dato a nessuno di cui non ti fidi, poiché chiunque conosca il tuo Xpub può ricavare tutte le tue chiavi pubbliche e quindi vedere ogni transazione passata e futura che tu possa fare. Le chiavi pubbliche estese sono utili per ricevere bitcoin direttamente su un cold storage wallet, poiché un utente può mantenere il proprio Xpub online per generare nuovi indirizzi mentre le proprie chiavi private rimangono offline.

Da un Xpub non si possono derivare chiavi private, quindi non c'è il rischio di perdere i propri bitcoin se il tuo Xpub è stato divulgato, anche se la tua privacy sarà compromessa. Tutte le chiavi Xpub inizieranno con le lettere "Xpub" seguite da una lunga stringa di lettere e numeri.

Con l'arrivo di SegWit, si sono resi disponibili nuovi formati di chiave pubblica estesa per derivare i nuovi tipi di indirizzi:

- ypub per derivare gli indirizzi P2SH-wrapped P2WPKH
- zpub per derivare indirizzi SegWit nativi, che usano script P2WPKH o P2WSH

Un modo semplice per distinguere tra Xpub, Ypub e Zpub è che gli indirizzi Xpub iniziano sempre con "1", gli indirizzi Ypub iniziano sempre con "3", mentre gli indirizzi Zpub iniziano sempre con "bc1".

A volte il termine Xpub viene genericamente utilizzato anche per indicare le chiavi pubbliche estese di tipo ypub e zpub.

L'Xpub è una metà della coppia di chiavi master, l'altra è una Xprv o chiave privata estesa.

ypub

Livello: avanzato

Argomento: tecnologia

ypub è una forma di chiave pubblica estesa xpub che segue un ulteriore standard definito in BIP 49.

Xpub, ypub e zpub permettono tutti ad un wallet di generare un albero deterministico di chiavi pubbliche, ma ogni forma di chiave pubblica estesa istruisce un wallet a derivare diversi tipi di indirizzi.

In particolare, ypubs istruisce un wallet a derivare indirizzi P2SH-wrapped P2WPKH.

Gli indirizzi P2WPKH sono indirizzi SegWit, ma per mantenere retro compatibilità, questi indirizzi SegWit sono wrappati in indirizzi P2SH per permettere ai vecchi wallet di inviare pagamenti verso indirizzi SegWit.

Dopo l'adozione di SegWit, è stato introdotto lo standard BIP49 che ha dato origine alla chiave Ypub. Una chiave Ypub è uguale a una chiave Xpub, ma segue il nuovo standard e ha un tipo di indirizzo P2SH-P2WPKH. Ypub è per wallet SegWit retrocompatibili.

Un modo semplice per distinguere tra Xpub, Ypub e Zpub:

- gli indirizzi Xpub iniziano sempre con **1**
- gli indirizzi Ypub iniziano sempre con **3**
- mentre gli indirizzi Zpub iniziano sempre con **bc1**

Zap

Livello: intermedio

Argomento: tecnologia

Gli Zap sono pagamenti sulla rete Lightning tramite il social network Nostr.
Non sono una parte fondamentale di Nostr, ma sono diventati abbastanza popolari tra gli utenti da essere rapidamente integrati nell'esperienza quotidiana di Nostr.

Gli zap sono una forma di micropagamenti che possono essere utilizzati per premiare i contenuti di alta qualità, incoraggiare la partecipazione alla community e supportare i creatori.
Gli Zap vengono effettuati utilizzando la rete Lightning, che è una rete di micropagamenti basata su Bitcoin che è molto veloce ed efficiente.

Gli Zap possono essere inviati a qualsiasi utente di nostr, anche se non sono amici o follower.
Per inviare un zap, è sufficiente fare clic sull'icona o pulsante Zap sotto il post di un utente, generalmente a forma di fulmine. Si aprirà una finestra pop-up in cui è possibile inserire l'importo dello zap e un messaggio opzionale. Il destinatario dello zap riceverà una notifica e potrà incassare l'importo dello zap sul suo wallet Bitcoin.

Per poter fare questo è necessario che il wallet e il client Nostr di chi effettua lo zap sia compatibile con gli Zap, e che il ricevente abbia specificato l'indirizzo lightning nel suo profilo Nostr.

Gli Zap sono un modo semplice e conveniente per mostrare il proprio apprezzamento per i contenuti di alta qualità e supportare i creatori. Sono una parte importante della community di nostr e stanno contribuendo a creare un ambiente più positivo e inclusivo.

I pagamenti zap su Nostr sono definiti dalle specifiche descritte nel documento NIP-57. Quando un utente effettua un pagamento zap su Nostr, Nostr genera una ricevuta in formato NIP-57 e la invia al destinatario. Il destinatario può quindi visualizzare la ricevuta sul proprio sito web o app.
NIP-57 crea due nuovi tipi di eventi nostr:

- 9734 è la zap request, la richiesta da parte del pagatore di una Lightning Invoice verso il wallet lightning del ricevente
- 9735 è una receipt (ricevuta) zap, che rappresenta la conferma dal wallet lightning del ricevente che l'invoice emessa in risposta alla richiesta dello zap è stata pagata.

Insieme, questi due tipi consentono ai client Nostr di richiedere invoice Zap dai server LNURL e di pagarle. La specifica NIP-57 descrive anche come i wallet Lightning che ricevono pagamenti Zap dovrebbero creare note da inviare ai relais di Nostr.

Zero Base Fee

Livello: avanzato

Argomento: tecnologia

Zero Base Fee è una iniziativa che promuove l'impostazione base_fee a 0 per migliorare le prestazioni di Lightning Network.

Quando viene fatto un pagamento su Lightning Network, il pagamento può attraversare diversi canali, potenzialmente decine di canali, e i suoi importi possono anche essere divisi su diversi percorsi, in un percorso chiamato MPP multi-path payment.

Calcolare il percorso più economico può essere una funzione complicata, e Rene Pickhardt e Stefan Richter hanno effettuato uno studio che ha rilevato che, se nella funzione di pagamento è inclusa una base_fee maggiore di 0, trovare il pagamento multiplo più economico è un problema NP-completo (nella teoria della complessità computazionale i problemi NP-completi sono i più difficili problemi nella classe NP "problemi non deterministici in tempo polinomiale").

Se la base_fee viene eliminata, i nodi possono calcolare questo problema di ottimizzazione. Il nuovo algoritmo di pathfinding di Rene e Stefans (noto anche come Pickhardt Payments) consentirebbe di inviare su Lightning Network

importi molto più elevati di quelli attuali.

Vengono chiamati Non-zero base fee i canali che non supportano il zero base fee routing.

ZeroMQ

Livello: avanzato

Argomento: tecnologia

ZeroMQ è un wrapper leggero attorno alle connessioni TCP, alla comunicazione inter-processo e alla memoria condivisa, che fornisce varie semantiche orientate ai messaggi come publish/subscribe, request/reply e push/pull.

Il demone Bitcoin Core può essere configurato per agire come un "border router" fidato, implementando il protocollo bitcoin di connessione relay, prendendo decisioni di consenso, mantenendo il database locale della blockchain, trasmettendo le transazioni generate localmente nella rete e fornendo un'interfaccia RPC interrogabile per interagire su base polled per richiedere dati relativi alla blockchain. Tuttavia, esiste solo un servizio limitato per notificare al software esterno eventi come l'arrivo di nuovi blocchi o transazioni.

La struttura ZeroMQ implementa un'interfaccia di notifica attraverso un insieme di notificatori specifici. Attualmente esistono notificatori che pubblicano blocchi e transazioni. Questa funzione di sola lettura richiede solo la connessione di una corrispondente porta di sottoscrizione ZeroMQ nel software ricevente; non è autenticata né vi è alcun coinvolgimento bidirezionale del protocollo. Pertanto, i sottoscrittori devono convalidare i dati ricevuti, poiché potrebbero essere non aggiornati, incompleti o addirittura non validi.

I socket ZeroMQ sono autocolleganti e autorigeneranti; in altre parole, le connessioni effettuate tra due endpoint saranno automaticamente ripristinate dopo un'interruzione e una delle due estremità può essere liberamente avviata o interrotta in qualsiasi ordine.

Poiché ZeroMQ è orientato ai messaggi, i sottoscrittori ricevono transazioni e blocchi tutti insieme e non hanno bisogno di implementare alcun tipo di buffering o riassemblaggio.

ZK

Acronimo di: Zero-Knowledge Proofs

Prova a conoscenza zero

Livello: avanzato

Argomento: tecnologia

Le Zero-Knowledge Proofs, o prove a conoscenza zero, sono un concetto crittografico che consente a una parte di dimostrare di avere una determinata informazione senza rivelare il contenuto specifico di quella informazione. In altre parole, una Zero-Knowledge Proof permette di dimostrare che si possiede una conoscenza senza doverla condividere con l'altra parte coinvolta nella transazione.

Nel contesto della crittografia, le Zero-Knowledge Proofs sono utilizzate per dimostrare la veridicità di una determinata affermazione senza rivelare le informazioni che la rendono vera. Ad esempio, supponiamo che Alice voglia dimostrare a Bob di conoscere la password di un account senza rivelare effettivamente la password stessa. Utilizzando una Zero-Knowledge Proof, Alice può dimostrare a Bob che sa qual è la password corretta, senza trasmetterla in chiaro.

Questi sistemi vengono usati da alcune criptovalute per poter memorizzare dati nella blockchain o fare transitare informazioni senza fornire il dettaglio sul loro contenuto ma consentendo ai partecipanti di verificare la loro legittimità, e trovano applicazioni in vari campi come la sicurezza informatica, la crittografia, i protocolli di autenticazione e la privacy. Possono essere utilizzate per verificare l'identità senza dover rivelare informazioni personali sensibili, per garantire la correttezza dei dati senza rivelarne il contenuto, o per dimostrare la validità di una transazione senza dover rivelare dettagli sensibili.

Le Zero-Knowledge Proofs sono basate su algoritmi crittografici, come le funzioni di hash crittografiche o gli impegni crittografici. Questi algoritmi consentono di generare prove che dimostrano la conoscenza di una determinata informazione senza rivelare direttamente quella informazione stessa.

In generale, le Zero-Knowledge Proofs rappresentano uno strumento potente per garantire la privacy e la sicurezza nelle comunicazioni e nelle transazioni, consentendo a due parti di scambiare informazioni in modo verificabile senza dover condividere i dettagli più sensibili.

Zk-Rollup

Livello: avanzato

Argomento: tecnologia

E' una tecnologia che può essere utilizzata per aggiungere scalabilità alla blockchain. Viene realizzata attraverso la fusione di transazioni off-chain che vengono scritte sulla blockchain in un'unica transazione tramite l'uso di Merkle Trees. Con ZK Rollup si possono mettere insieme migliaia di operazioni off-chain, creare una prova che queste operazioni sono tutte valide (i proprietari delle risorse firmano le operazioni), e pubblicare la prova sulla blockchain, dove viene verificata da uno smart contract. Durante questo processo, le risorse dell'utente on-chain sono conservate nello smart contract e possono essere rilasciate solo dopo che una prova valida che include le risorse è stata pubblicata in un batch

Zk-Snarks

Acronimo di: Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

Livello: avanzato

Argomento: tecnologia

noto anche come NIZK, o zk-STARK sono prove a conoscenza zero che non richiedono alcuna interazione tra il prover e il verificatore

ZKCP

Acronimo di: Zero-Knowledge Contingent Payment

Livello: avanzato

Argomento: tecnologia

ZKCP, Zero-Knowledge Contingent Payment si traduce in italiano come "Pagamento Contingente a Conoscenza Zero".

ZKCP è un protocollo di transazione che permette a un acquirente di acquistare informazioni da un venditore utilizzando Bitcoin in modo privato, scalabile, sicuro e senza dover fidarsi di nessuno: le informazioni desiderate vengono trasferite solo se il pagamento viene effettuato.
L'acquirente e il venditore non devono fidarsi l'uno dell'altro né dipendere da un'arbitrato da parte di terze parti.

ZKCP funziona utilizzando una tecnica crittografica chiamata "prova a conoscenza zero". Una prova a conoscenza zero consente a una persona di dimostrare a un'altra persona di conoscere un segreto senza rivelare il segreto stesso.

In un pagamento contingente a conoscenza zero, l'acquirente e il venditore utilizzano una prova a conoscenza zero per dimostrare di rispettare le loro rispettive parti dell'accordo. L'acquirente dimostra di possedere Bitcoin sufficienti per effettuare il pagamento e il venditore dimostra di possedere le informazioni che desidera vendere.

Una volta che entrambe le parti hanno dimostrato di rispettare le loro parti dell'accordo, le informazioni vengono trasferite all'acquirente e il pagamento viene trasferito al venditore.

zpub

Livello: avanzato

Argomento: tecnologia

zpub è una forma di chiave pubblica estesa, o xpub, che segue un successivo standard definito in BIP 84.

Xpub, ypub e zpub permettono tutti ad un portafoglio di generare un albero deterministico di chiavi pubbliche, ma ogni forma di chiave pubblica estesa istruisce un portafoglio a derivare diversi tipi di indirizzi.

In particolare, zpubs istruisce un portafoglio a derivare indirizzi SegWit nativi, che usano script P2WPKH o P2WSH.

P2WPKH è il tipo di indirizzo SegWit più comune. A differenza degli indirizzi P2SH-wrapped P2WPKH, che sono generati da ypub, gli indirizzi P2WPKH non sono retro compatibili.

Dopo la Xpub e la Ypub, la nuova chiave pubblica estesa si chiama Zpub. Come il suo predecessore, la Zpub segue lo standard BIP49, ma il tipo di indirizzo è P2WPKH. Zpub è destinato ai portafogli SegWit nativi compatibili.

Un modo semplice per distinguere tra Xpub, Ypub e Zpub:

- gli indirizzi Xpub iniziano sempre con **1**
- gli indirizzi Ypub iniziano sempre con **3**
- mentre gli indirizzi Zpub iniziano sempre con **bc1**