MODULO 3:

Blockchain, Tipi di Blockchain, Mining digitale, Transazioni

Come funziona la blockchain

La Blockchain è un tipo di rete distribuita che consente lo sviluppo di tecnologie come le criptovalute e quella che chiamiamo Internet del valore. Consente la creazione di un registro distribuito su una rete di computer senza la necessità di un server o di un database centrale. L'aggiornamento e la gestione di questo registro possono essere effettuati solo tramite il consenso di tutti i partecipanti alla rete.

Per questo motivo, la potenza di calcolo di tutti i nodi della rete viene utilizzata non solo per immettere informazioni, ma anche per proteggerle da modifiche non autorizzate. Di conseguenza, la blockchain consente livelli di sicurezza molto elevati rispetto ad altre tecnologie.

Affinché la tecnologia blockchain funzioni, è innanzitutto necessario creare un software specifico. Questo software consente ai computer di creare la rete che farà funzionare la blockchain in modo distribuito, proprio come il software alla base di Bitcoin e altre criptovalute. Generalmente, questo software è open source e protetto da licenze di software libero. Ciò significa che è pubblico, trasparente e può essere utilizzato, revisionato e contribuito da chiunque.

Poiché non dispone di un database o di un server centralizzato, una rete blockchain è caratterizzata da una rete distribuita. Ciò significa che le informazioni vengono replicate su tutti i computer della rete.

Se più del 50% dei computer in quella rete blockchain non appartiene alla stessa persona o azienda, possiamo dire che la rete è decentralizzata. Ciò significa che non ha un "centro di emissione, controllo o potere" centrale.
In sostanza, una rete blockchain è semplicemente un database che consente agli utenti di leggere e scrivere nuovi record, senza poter modificare quelli già esistenti. Tutti i record memorizzati al suo interno sono collegati tra loro tramite calcoli matematici altamente avanzati, rendendo impossibile aggiungere elementi incoerenti con i record esistenti.

Come si costruisce una blockchain?

La costruzione e il funzionamento della blockchain dipendono da una serie di elementi che esamineremo di seguito:

Blocchi

Un blocco è un insieme di transazioni confermate e informazioni aggiuntive incluse nella blockchain. Ogni blocco della catena (ad eccezione del blocco generatore, che dà inizio alla catena) è costituito da:

- Un codice alfanumerico che collega al blocco precedente;
- Il “pacchetto” di transazioni che include (il cui

numero è determinato da diversi fattori);
- Un altro codice alfanumerico che collegherà al blocco successivo.

Il blocco in corso tenta di determinare il terzo punto di cui abbiamo parlato attraverso calcoli. Si tratta di codice che segue regole specifiche per essere valido e può essere ottenuto solo attraverso test continui. Ma come vengono generate queste regole?

Minatori

I miner sono computer dedicati o apparecchiature specializzate che forniscono potenza di calcolo (o potenza di mining) alla rete Bitcoin. Questa potenza viene utilizzata per verificare le transazioni. Ogni volta che qualcuno completa un blocco, riceve una ricompensa in bitcoin e/o per ogni transazione completata.

Nodi

Un nodo è un computer/chip connesso alla rete Bitcoin tramite un software che memorizza e distribuisce una copia aggiornata della blockchain in tempo reale. Ogni volta che un blocco viene confermato e aggiunto alla catena, viene comunicato a tutti i nodi e aggiunto alla copia memorizzata da ciascun nodo.

Uno degli aspetti più intriganti del protocollo Bitcoin è che ogni unità non è un file nel senso tradizionale del

termine, inviato come un film o una canzone, simile a un protocollo P2P come BitTorrent. Si tratta invece di una registrazione del cambio di proprietà di una quantità specifica di bitcoin sulla blockchain. Il software di nodo più comune sulla rete Bitcoin è Bitcoin Core.

Quasi tutte le criptovalute seguono questa struttura tripartita, ognuna con le sue peculiarità. Ma questo semplice funzionamento garantisce la massima sicurezza garantita dalla blockchain.

Utilità della tecnologia blockchain

Gli utilizzi della blockchain sono molteplici. Infatti, è già implementata in molteplici settori in una corsa tecnologica che cambierà per sempre aspetti essenziali della nostra vita individuale e collettiva.

Proprio come Internet ha rivoluzionato il modo in cui creiamo, trasmettiamo e consumiamo informazioni, con la tecnologia blockchain siamo sull'orlo di quella che viene chiamata Internet del valore o Internet del denaro.

La tecnologia blockchain è essenziale per la creazione di criptovalute. Queste possono essere utilizzate per trasferire valore tra persone in tutto il mondo. Oltre a digitalizzare la proprietà di qualsiasi bene di valore (tangibile o intangibile), ci consente, tra le altre cose, di creare registri immutabili di beni e proprietà digitali che possono essere trasferiti tra individui senza la

necessità di un intermediario di fiducia (banche, notai, ecc.), come è avvenuto finora.
La blockchain e il suo funzionamento rendono questa tecnologia una delle più sicure disponibili. Tutto questo grazie alla sua struttura distribuita, all'uso di una crittografia avanzata e a un potente sistema di consenso che garantisce l'integrità dei dati.
L'ulteriore esplorazione e sviluppo di questa tecnologia ci porterà a un punto in cui potremo interconnettere il mondo in modo più efficace, il tutto senza compromettere la nostra privacy o la sicurezza dei nostri sistemi e dati.

Tipi di blockchain

Attualmente esistono diversi tipi di blockchain, ognuno con capacità e caratteristiche uniche per soddisfare esigenze diverse. Questi tipi di blockchain sono pubblici, privati e ibridi o federati.

La tecnologia blockchain si è evoluta in modo significativo sin dal suo inizio, un'evoluzione che ha attirato l'attenzione di molti stakeholder in tutto il mondo. Inizialmente, i principali stakeholder erano individui che ne prevedevano l'impatto trasformativo e rivoluzionario. Si trattava di una tecnologia pubblica, accessibile a tutti, sia per il miglioramento che per la partecipazione attiva. Tuttavia, ci è voluto del tempo prima che aziende e governi iniziassero a interessarsi alla tecnologia per utilizzarla nei propri progetti.

Ma gli interessi delle aziende e dei governi differiscono da quelli delle comunità aperte. Questa prospettiva ha dato vita a progetti blockchain diversi da qualsiasi cosa si conoscesse in precedenza. È così che sono nate le blockchain private e le blockchain ibride o federate. In questo modulo, spiegherò ciascuno dei tipi di blockchain attualmente esistenti, menzionandone il potenziale e le caratteristiche uniche.

Blockchain pubblica

Questo è stato il primo tipo di blockchain e si riferisce a blockchain accessibili al pubblico tramite Internet. Esempi di questo tipo di blockchain includono Bitcoin, Dash, Monero e Zcash. Queste blockchain mantengono i loro dati, software e sviluppo aperti al pubblico, consentendo a chiunque di esaminarli, verificarli, svilupparli o migliorarli.
Per raggiungere questo obiettivo, le blockchain pubbliche adottano misure di sicurezza che garantiscono che nessun malintenzionato possa facilmente interromperne il funzionamento. È qui che entrano in gioco la tolleranza ai guasti bizantina, i robusti protocolli di consenso e le protezioni contro attacchi DDoS, attacchi del 51% e double spending. In breve, viene implementata qualsiasi misura che contribuisca a migliorare la sicurezza della rete. L'obiettivo finale è mantenere la rete operativa e

preservarne la decentralizzazione.
Tra le caratteristiche di questa tipologia di rete possiamo citare:
Le blockchain pubbliche consentono a chiunque di partecipare. Che si tratti di utenti, miner o amministratori di nodi, chiunque può accedere e partecipare alla rete senza alcuna restrizione.

La rete opera in modo completamente trasparente e aperto. I dati della blockchain sono accessibili a tutti senza restrizioni fin dal suo inizio. Chiunque può esaminare o verificare il funzionamento della rete e del suo software.

Non esistono entità centralizzate. Le reti pubbliche sono completamente decentralizzate e non esiste un'autorità centrale che ne regoli il funzionamento.

Il mantenimento finanziario della blockchain dipende dal sistema integrato al suo interno. Questo sistema economico si basa generalmente sul mining e sulla riscossione di commissioni per ogni transazione effettuata all'interno della rete.

Blockchain privata o autorizzata

Successivamente, con l'evoluzione e l'espansione della tecnologia blockchain, molte aziende si sono interessate ad essa. Ciò ha portato allo sviluppo di soluzioni blockchain private o permissioned. Questo tipo di blockchain presenta generalmente gli stessi

elementi di una blockchain pubblica, ma a differenza di quest'ultima, le blockchain permissioned si basano su un'autorità centrale che controlla tutte le azioni all'interno della blockchain.

Questa unità centrale è ciò che garantisce l'accesso degli utenti, oltre a controllarne le funzioni e i permessi all'interno della blockchain. Si tratta generalmente di opzioni di sviluppo software proprietario, sebbene esistano anche software open source. Uno degli sviluppi blockchain privati più importanti nel mondo delle criptovalute è Hyperledger. Questo progetto, avviato dalla Linux Foundation e da diverse aziende del settore tecnologico, è il principale esempio di blockchain privata. Possiamo anche citare Corda di R3 o Quorum di JPMorgan.

Tra le caratteristiche di questa tipologia di rete possiamo citare:

- L'accesso alla rete è limitato agli elementi che possono essere autorizzati solo dall'unità di controllo centrale;
- L'accesso al registro delle transazioni o a qualsiasi altra informazione generata dalla blockchain è privato;
- Il mantenimento finanziario di una blockchain dipende generalmente dall'azienda che supporta il progetto. Le blockchain private spesso non utilizzano criptovalute né si occupano di mining.

Ogni scenario ed esigenza è diverso; pertanto, devono

essere affrontati in modo specifico. I tipi di blockchain menzionati qui sono:

Blockchain ibrida o federata

Questo tipo di blockchain è una fusione di blockchain pubbliche e private. È un tentativo di sfruttare il meglio di entrambi i mondi. In queste blockchain, la partecipazione alla rete è privata. Ciò significa che l'accesso alle risorse della rete è controllato da una o più entità. Tuttavia, il registro è accessibile al pubblico. Ciò significa che chiunque può esplorare, blocco per blocco, tutto ciò che accade sulla blockchain.

Ad esempio, queste tipologie di reti blockchain sono molto utili per governi o aziende che desiderano archiviare o condividere dati in modo sicuro. Un caso d'uso ideale sta emergendo nel settore sanitario, dove la blockchain sta iniziando a essere utilizzata per archiviare i dati provenienti dalle linee di produzione dei farmaci. I dati archiviati possono essere esaminati dalle autorità competenti per controllarne la qualità, sia a livello aziendale che governativo. L'obiettivo dell'implementazione di questo modello blockchain è mantenere un elevato livello di trasparenza e fiducia.
Tra le caratteristiche di questa tipologia di rete possiamo citare:

- L'accesso alla rete è limitato agli elementi che possono essere autorizzati solo dalle altre unità di

controllo.

- L'accesso al registro delle transazioni o a qualsiasi altra informazione generata dalla blockchain è pubblico.
- Non è coinvolto alcun mining o criptovaluta. Il consenso di rete viene raggiunto attraverso altri mezzi che garantiscono l'accuratezza dei dati.
- È parzialmente decentralizzato, il che comporta un maggiore livello di sicurezza e trasparenza.

COS'È IL MINING DI CRIPTOVALUTE?

Il mining di criptovalute è uno degli elementi chiave che consentono alle criptovalute di funzionare come una rete peer-to-peer decentralizzata, senza la necessità di un'autorità centrale terza.
Si tratta di un processo in cui le transazioni tra utenti vengono verificate e aggiunte al registro pubblico della blockchain, nonché di un processo utilizzato per introdurre nuove monete nell'offerta circolante esistente.

COME FUNZIONA?

Un miner è un nodo della rete che raccoglie le transazioni e le organizza in blocchi. Ogni volta che si verificano transazioni, i nodi di mining le ricevono e le verificano, le aggiungono al pool di memoria e iniziano ad assemblarle in un blocco di più transazioni.

Il primo passo in un processo di block mining è raggruppare ogni transazione nel pool di memoria.
Prima che il processo abbia inizio, il nodo di mining aggiunge una transazione in cui viene inviata la ricompensa per il mining. Questa transazione è nota come transazione "coinbase"; è una transazione in cui le monete vengono create secondo regole matematiche del protocollo e, nella maggior parte dei casi, è la prima transazione in un nuovo blocco.
Una volta eseguita l'hashing di ogni transazione, questi hash vengono organizzati in un elemento chiamato “Albero di Merkle” (o “Albero Hash”); ció significa che gli hash vengono disposti a coppie e concatenati fino a raggiungere "la cima dell'albero", chiamata anche “Hash Radice” o “Radice di Merkle”.
L'Hash Radice, insieme all'hash del blocco precedente e a un numero casuale chiamato “Nonce”, vengono inseriti nell'intestazione del blocco. L'intestazione del blocco viene elaborata come hash e produce un output che funge da identificatore del blocco.
L'hash identificatore del blocco deve essere inferiore a un certo valore target impostato dal protocollo, ragion per cui l'hash dell'intestazione del blocco inizia con un certo numero di zeri.
Questo valore target, noto anche come “difficoltà di hash”, è scalabile, garantendo che la velocità con cui vengono creati nuovi blocchi rimanga proporzionale alla quantità di potenza di hashing sulla rete.

I miner cercano l'hash dell'intestazione ripetutamente finché uno di loro non ne produce finalmente uno. Quando viene trovato un hash valido, il nodo fondatore trasmette il blocco alla rete. Tutti gli altri nodi verificano quindi l'hash, aggiungono il blocco alla propria copia della blockchain e continuano a estrarre il blocco successivo.
Puó succedere che due miner emettano un blocco valido contemporaneamente e la rete si ritrova con due blocchi “concorrenti”. I miner iniziano a minare il blocco successivo in base al blocco ricevuto per primo, ma la competizione tra questi blocchi continua finché il blocco successivo non viene minato in base a uno dei blocchi concorrenti. Il blocco abbandonato è chiamato “Blocco Orfano” o “Blocco Obsoleto”.

Introduzione ai pool di mining

Il mining è una componente integrante della sicurezza della blockchain. Attraverso la POW, durante l'elaborazione computazionale dell’hash con determinate proprietà, i partecipanti sono in grado di proteggere le reti di criptovalute senza la necessità di un'autorità centrale. Quando Bitcoin fu lanciato originariamente nel 2009, chiunque avesse un PC normale poteva competere con altri minatori cercando di “indovinare” l'hash valido del prossimo blocco. Questo perché la difficoltà di estrazione era bassa.

Non c'era molto hashrate sulla rete. Pertanto, non era necessario hardware specializzato per aggiungere nuovi blocchi alla blockchain.
Logicamente, chi riusciva a calcolare più hash al secondo trovava più blocchi e questo avrebbe causato un cambiamento radicale nell'ecosistema. Nella loro lotta per ottenere un vantaggio competitivo, i miner finivano per entrare in una sorta di "corsa agli armamenti".
Dopo aver esaminato diversi tipi di hardware (CPU, GPU, FPGA), i minatori di Bitcoin alla fine adottarono gli ASIC – Circuiti integrati specifici per applicazione. Questi dispositivi computazionali non permettono di navigare sul web o twittare foto di gatti, ma come suggerisce il nome, sono progettati per svolgere un unico compito: calcolare gli hash. Essendo stati progettati per questo scopo specifico, lo svolgono incredibilmente bene; così bene che l'utilizzo di altri tipi di hardware per minare Bitcoin è diventato piuttosto raro.

Cos'è un mining pool?
Un buon hardware ti aiuterà solo fino a un certo punto. Potresti averne diversi in funzione e di grande potenza, e saresti ancora solo una goccia nell'oceano dell'attività Bitcoin.
Le possibilità di minare un blocco sono piuttosto rare,

anche se hai speso un sacco di soldi in hardware e nell'elettricità necessaria per mantenerli in funzione.
Non vi è alcuna garanzia circa i tempi di ricezione del pagamento di ricompensa per blocco e nemmeno *la certezza* che alla fine verrai pagato. Se quello che cerchi è un reddito fisso, avrai molto più successo in un mining pool.
Supponiamo che tu e altri nove partecipanti abbiate ciascuno lo 0,1% della potenza di hash totale della rete. Ciò significa che, in media, vi aspettereste di trovare un blocco ogni mille. Sulla base di una stima di 144 blocchi estratti al giorno, probabilmente ne trovereste uno ogni settimana. A seconda della vostra liquidità e del vostro investimento in hardware ed elettricità, questo approccio di "mining in solitaria" potrebbe essere una strategia praticabile.
Ma cosa succede se questo reddito non è sufficiente a generare profitti? In tal caso, potreste unire le forze con gli altri nove partecipanti che abbiamo menzionato. Unendo la potenza di hash di ognuno, otterreste l'1% del tasso di hash della rete. Ciò significa che, statisticamente, potreste trovare uno o due blocchi al giorno e dividerne la ricompensa. In breve, abbiamo appena descritto cos'è un mining pool. Questi sono ampiamente utilizzati oggi perché garantiscono ai loro membri un flusso di reddito più costante.

Come funzionano le mining pool?

In genere, un mining pool designa un coordinatore, che sarà responsabile dell'organizzazione dei minatori. Questo coordinatore garantirà che i minatori utilizzino valori diversi per il calcolo, in modo da non sprecare potenza di hash cercando di creare gli stessi blocchi. I coordinatori sono anche responsabili della divisione delle ricompense e del loro pagamento ai partecipanti.
Per calcolare il lavoro svolto da ciascuno per trovare un minatore e ricompensarlo adeguatamente, si utilizzano diversi metodi; vediamoli qui sotto.

Pool di mining Pay-Per-Share (PPS):

Uno dei sistemi di compensazione più tipici è il “Pagamento per azione” *(PPS).* Con questo sistema riceverai un importo fisso per ogni "quota" inviata.
Una quota è un hash utilizzato per tracciare il lavoro di ciascun miner. L'importo pagato per ogni quota è nominale, ma si accumula nel tempo. Si noti che una quota non è un hash valido all'interno della rete. È semplicemente un hash che soddisfa le condizioni stabilite dal mining pool.
Nel PPS, si riceve una ricompensa se il pool risolve un blocco. Il gestore del pool si assume il rischio, quindi è probabile che addebiti una commissione sostanziale, anticipata dagli utenti o detratta dall'eventuale ricompensa per il blocco.

Pool di mining Pay-Per-Last-N-Shares (PPLNS)

Un altro schema popolare è il Pay-Per-Last-N-Shares (PPLNS). A differenza del PPS, il PPLNS premia i miner solo quando il pool mina con successo un blocco. Quando il pool trova un blocco, controlla l'ultima share. *N* è il Numero di azioni inviate (N varia a seconda del pool). Per ottenere il pagamento, dividi il numero di azioni inviate per N, quindi moltiplica il risultato per la ricompensa del blocco (meno la commissione dell'operatore).

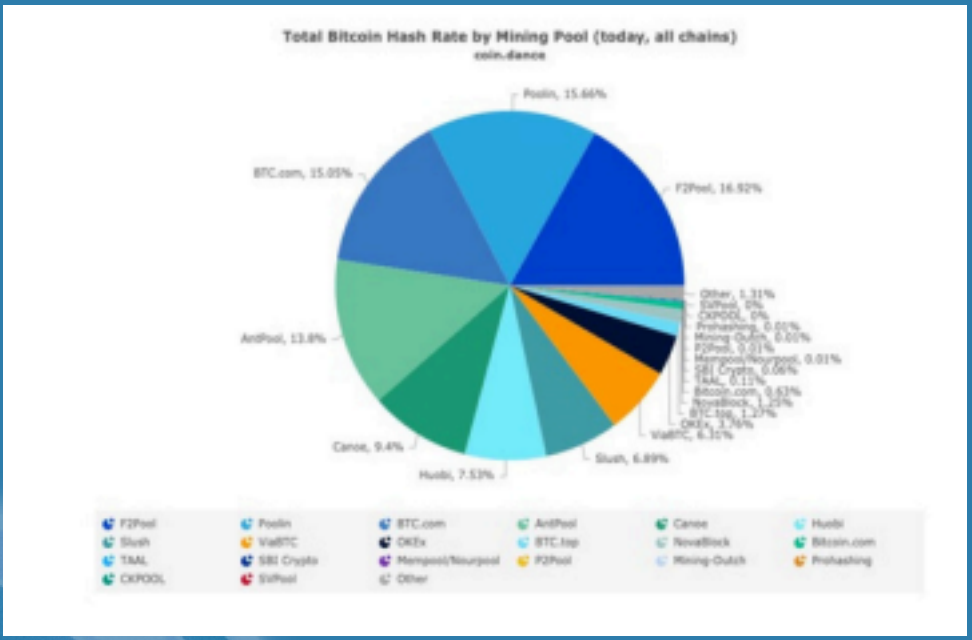
Facciamo un esempio. Se la ricompensa attuale per blocco è di 3,125 BTC (ipotizzando che non ci siano commissioni di transazione) e la commissione dell'operatore è del 20%, la ricompensa disponibile per i miner è di 2,5 BTC. Se N fosse 1.000.000 e tu facilitassi 50.000 azioni, riceveresti il 5% della ricompensa disponibile (0,125 BTC).

Esistono diverse varianti di questi due schemi, ma questi sono quelli di cui potresti sentir parlare più spesso. Tieni presente che, mentre parliamo di Bitcoin, anche le criptovalute Proof-of-Work più popolari dispongono di mining pool.

I mining pool rappresentano una minaccia per la decentralizzazione?

Il motivo per cui bitcoin è così potente non è forse perché non è controllato da una singola entità? Cosa succede se qualcuno ottiene la maggior parte del

potere di hashing?
Queste sono domande molto valide. Se una singola entità può acquisire il 51% della potenza di hash della rete, può lanciare un attacco del 51%. Ciò le consentirebbe di censurare le nuove transazioni e di annullare quelle vecchie. Un attacco del genere potrebbe causare danni ingenti a un ecosistema di criptovalute. I mining pool aumentano il rischio di un attacco del 51%? La risposta è: forse, ma è improbabile.



Ripartizione dell'hash rate di 24 ore per pool al 16 aprile 2020. Fonte:coindance.com

In teoria, i quattro principali pool potrebbero collaborare per dirottare la rete. Tuttavia, ciò non avrebbe molto senso. Anche se riuscissero a portare a termine un attacco, il prezzo di Bitcoin crollerebbe probabilmente, poiché le loro azioni minerebbero il

sistema. Di conseguenza, tutte le monete acquisite perderebbero valore.

Inoltre, i pool di mining non possiedono necessariamente l'attrezzatura necessaria per il mining. Le entità puntano le loro macchine al server del coordinatore, ma sono libere di migrare verso altri pool. Mantenere l'ecosistema decentralizzato è nell'interesse sia dei partecipanti che dei gestori dei pool. Dopotutto, guadagnano solo se il mining rimane redditizio.

Ci sono stati alcuni casi in cui i pool di mining hanno raggiunto dimensioni che potrebbero essere considerate preoccupanti. In genere, il pool (e i suoi miner) adottano misure per ridurre l'hash rate.

In un mondo ideale, l'attività di mining di Bitcoin, Bitcoin non è gestito dai miner, ma dagli utenti. sarebbe ancora più decentralizzato. Per il momento, tuttavia, è quello che potremmo definire "sufficientemente decentralizzato". In ogni caso, nessuno trarrebbe vantaggio dal fatto che un singolo pool catturi la maggior parte dell'hashrate nel lungo periodo.

Transazioni Bitcoin: come funzionano?

Le transazioni di criptovalute sono una parte essenziale che ci permette di utilizzare e gestire i nostri fondi in modo rapido, sicuro e semplice. Scopri come funzionano e le infinite possibilità che ci offrono.

Le transazioni (a volte chiamate anche TX) sono una componente fondamentale e indispensabile nel funzionamento delle criptovalute e rappresentano la colonna portante di tutto questo sistema di pagamento crittografico. Sono ciò che ci consente di usare e gestire i nostri fondi in modo rapido, sicuro e facile.

Per questo motivo, sapere cos'è una transazione e come funziona è di vitale importanza per comprendere come operano le criptovalute.

In termini semplici, una transazione è un invio o un trasferimento di valore tra due parti. Nel caso di Bitcoin, queste transazioni possono essere intese come trasferimenti di bitcoin tra persone che utilizzano la rete. Queste transazioni non sono altro che registrazioni memorizzate all'interno della blockchain di Bitcoin, cioè un flusso di informazioni.

In termini tecnici, una transazione Bitcoin è un messaggio digitale strutturato, firmato crittograficamente, che consuma uno o più output non spesi (UTXO), crea uno o più nuovi output e viene validato dalla rete e registrato nella blockchain, ridefinendo la proprietà di determinati output. Quindi, le transazioni in Bitcoin sono semplicemente messaggi contenenti informazioni, che possono essere programmati e firmati digitalmente tramite la crittografia e inviati a tutta la rete per la loro validazione. Questa è la ragione per cui si dice che Bitcoin è denaro programmabile.

Inoltre, poiché le transazioni sulla rete Bitcoin sono pubbliche, possono essere facilmente trovate all'interno della blockchain. In essa è possibile verificare tutte le transazioni, fin dalla creazione del primo bitcoin.

Come funzionano le transazioni in Bitcoin

Le transazioni di bitcoin sono intese come l'invio di bitcoin da una persona a un'altra utilizzando la rete Bitcoin. A questo punto, tutte queste transazioni non sono altro che registri memorizzati nella blockchain. Lo stesso principio si applica anche al resto delle criptovalute PoW.

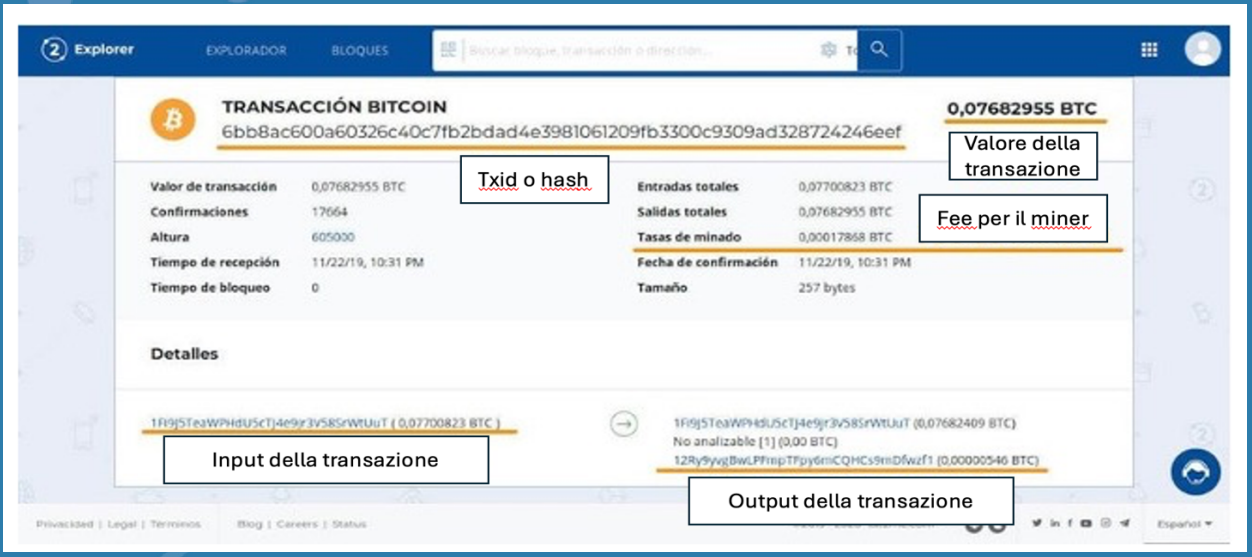
Per effettuare tali transazioni, è necessario disporre di un client per la criptovaluta, meglio conosciuto come portafoglio o wallet. Questi non sono altro che un software che ci permette di gestire i nostri fondi. Grazie a essi possiamo inviare e ricevere criptovalute, cioè effettuare o ricevere transazioni che hanno origine in una determinata blockchain.

Per capire come funzionano le transazioni, è importante prima sapere come sono strutturate.

Input (entrate): Gli input sono riferimenti a un'uscita di una transazione passata che non è stata utilizzata in nessun'altra transazione. Questi ci permettono di confermare la provenienza degli asset che saranno impiegati in una transazione e contengono l'indirizzo dove i bitcoin erano stati ricevuti originariamente.

Output (uscite): Gli output contengono l'indirizzo a cui viene effettuato il trasferimento e la quantità inviata. Inoltre contengono gli indirizzi di resto o di ritorno, dove vengono inviati eventuali "resti" della transazione. Pertanto, una transazione può avere più di un output.
Identificatore (TXid): Ogni transazione eseguita avrà il proprio hash. Questo hash viene generato a partire dagli input e dagli output ed è il valore che permette di identificare una transazione in modo unico e irripetibile all'interno della blockchain.
Commissione (fee): La fee è il piccolo pagamento che i miner ricevono per processare una transazione. Così, il miner che genera un nuovo blocco riceverà una fee per ogni transazione processata all'interno di quel blocco. La commissione non appare esplicitamente nel contenuto di una transazione, cioè non è associata a nessun output, poiché non si sa quale miner la riceverà. Per questo motivo, viene lasciata una certa quantità non associata a nessun output, che sarà considerata come commissione per i miner.

Nell'immagine seguente possiamo vedere ciascuna di queste sezioni all'interno di una transazione di Bitcoin.



Funzionamento di una transazione.

Le transazioni di criptovalute hanno tutta la struttura di base mostrata in precedenza. Questa struttura ha un design curioso, con input e output, ma con un obiettivo molto preciso: garantire la sicurezza. In ogni momento, questi dati passano attraverso un processo crittografico di hash e crittografia asimmetrica. È proprio questo processo che permette di assicurare e validare correttamente le informazioni.

In Bitcoin, questo processo che rende tutto ciò possibile è gestito dal Bitcoin scripting. Si tratta di un potente linguaggio di programmazione che permette a

```
OP_DUP  OP_HASH160
b2089ebaad05c87a6d714cc33fbaa8cf181a4e30      OP_EQUALVERIFY
OP_CHECKSIG
```

Bitcoin di avere un enorme potenziale. E così, anche se il suo potenziale è molto grande, la grande maggioranza delle transazioni in Bitcoin attualmente

segue proprio questo schema.
Questo schema si ripete, fino a un certo punto, anche in altre criptovalute, ma ovviamente ognuna di esse ha le proprie particolarità, che possono migliorare o semplificare la gestione delle transazioni.
Esempio:
Immagina che Maria possieda il controllo di un indirizzo con 1 bitcoin. Se volesse inviare a Pedro solo 0,3 bitcoin e non esistesse il concetto di input, il sistema non avrebbe modo di sapere quale parte di quell'1 bitcoin corrisponde ai 0,3 inviati, rischiando che la stessa somma possa essere riutilizzata.
Per questo esiste il concetto di input, ai quali vengono associati i bitcoin che arrivano a un indirizzo. In questo modo, si selezionano gli input sufficienti per raggiungere l'importo desiderato.
Se per inviare 0,3 bitcoin fosse necessario selezionare 3 input da 0,12 ciascuno, il totale sarebbe 0,36 bitcoin. I restanti 0,06 bitcoin vengono inviati a un indirizzo proprio, indicato come output insieme all'indirizzo del destinatario dei 0,3 bitcoin.
In altre parole, avremmo questo scenario di input e output:

L'indirizzo proprio a cui vengono inviati i 0,06 BTC rimanenti può essere lo stesso indirizzo associato agli input oppure un nuovo indirizzo. Questo viene

chiamato indirizzo di resto o indirizzo di ritorno, ed è lì che vengono inviati i “resti”.
Quindi, avendo chiari questi punti, per effettuare una transazione in Bitcoin è necessario:
Selezionare gli input sufficienti per coprire l’importo che si vuole inviare.
Determinare gli output, cioè l’indirizzo del destinatario e, se necessario, l’indirizzo di resto per ricevere eventuali “resti” della transazione.
Calcolare la fee da inviare ai miner, lasciando tale importo non associato a nessun output, in modo che venga riconosciuto come commissione.
Firmare la transazione con la chiave privata associata agli input, garantendo così l’autenticità e l’autorizzazione del trasferimento.
Trasmettere la transazione alla rete Bitcoin, dove i nodi e i miner la verificheranno e la includeranno in un blocco della blockchain.
In questo modo, ogni transazione è sicura, tracciabile e non può essere duplicata o spesa due volte.
È importante capire anche che in una stessa transazione possono esserci tante entrate provenienti dallo stesso indirizzo, o da indirizzi diversi, quante se ne desideri. Lo stesso vale per le uscite. Questo permette di effettuare, in una sola transazione, molti invii a persone diverse pagando una sola commissione ai miner. Questa funzionalità viene sfruttata da alcuni portafogli per risparmiare sui costi.

Il modo in cui il protocollo ricompensa i miner deriva dai fondi che non vengono assegnati a nessun indirizzo. Tutti i bitcoin rimanenti in una transazione che non vengono assegnati a nessun indirizzo vengono trattenuti dal miner che trova il blocco contenente la tua transazione e sono impossibili da recuperare.
Quindi, avendo chiari questi punti, per effettuare una transazione sulla rete Bitcoin, il mittente deve avere accesso sia agli indirizzi pubblici sia alle chiavi private associate a quei bitcoin. Queste ultime non sono altro che un insieme casuale di numeri e lettere senza un modello definito.
La chiave privata è ciò che ci permette di firmare e inviare una transazione come proprietari di determinati bitcoin, mentre l'indirizzo pubblico funziona come un indirizzo e-mail o un numero di conto bancario, a cui inviare o da cui ricevere la transazione.

Tipi di transazioni esistenti in Bitcoin: **Coinbase**
Una **transazione coinbase** è quella che permette ai miner di generare o attivare nuove criptovalute, con le quali possono ricevere le ricompense della **mining**.
Nel caso di Bitcoin, la prima transazione effettuata fu chiamata **coinbase**. Non fu effettuata da una persona all'altra, ma piuttosto dalla rete stessa come **transazione generatrice**, tramite la quale fu "dato vita" all'intero sistema Bitcoin.

I nodi miner possono aggiungere solo una transazione coinbase per ogni nuovo blocco generato. In questo modo il sistema garantisce che il miner riceva soltanto la ricompensa che gli spetta e che vengano immesse in circolazione nuove monete che non erano mai state precedentemente nella blockchain.

Nella coinbase vengono incluse anche le commissioni delle transazioni elaborate dal miner. Pertanto, questo tipo di transazione contiene la somma della ricompensa per il mining del blocco più le commissioni delle transazioni processate. Generalmente, la coinbase è la prima transazione inserita all'interno di un nuovo blocco.

UTXO

Le UTXO sono le monete non spese. Nel protocollo Bitcoin, le entrate delle transazioni (inputs) vengono chiamate anche UTXO di una transazione precedente, cioè uscite di una transazione non ancora spese o utilizzate. Contengono fondamentalmente il resto derivante da una transazione.

Ad esempio, se hai 1 BTC nel tuo portafoglio, è probabile che questi provengano da diverse UTXO, ad esempio 4 UTXO da 0,25 BTC ciascuna. Se desideri spendere 0,30 BTC per un prodotto, noterai che non possiedi alcuna UTXO con quell'importo esatto. Anche se il portafoglio mostrerà un saldo totale di 1 BTC per semplificare le cose.

In realtà, le UTXO non possono essere divise. Perciò,

quando effettui un pagamento di 0,30 BTC, ciò che stai realmente inviando è 0,50 BTC (2 UTXO in questo caso). Il tuo portafoglio creerà quindi due uscite: una per il commerciante a cui paghi 0,30 BTC, e una per te con 0,20 BTC come resto.

La presenza delle UTXO è ciò che permette il funzionamento delle transazioni Child Pays for Parents (CPFP). Si tratta di una transazione con una commissione di mining maggiore, in cui vengono movimentate le UTXO di una transazione non confermata, in modo da far confermare più rapidamente la transazione "padre" che le ha generate.

Processo per creare transazioni che inviano criptovalute

Per inviare criptovalute servono due elementi: un indirizzo e una chiave privata. Entrambi sono gestiti dal portafoglio o wallet di criptovalute.

In primo luogo, l'indirizzo è in realtà la chiave pubblica della chiave privata del proprietario delle criptovalute. Può essere, ad esempio, la chiave che dà accesso a determinati bitcoin. Ciò che rende queste chiavi così sicure è che entrambe sono sequenze di lettere e numeri generate mediante matematica avanzata e casuale.

L'indirizzo (la chiave pubblica) segue un modello determinato e unico, che può iniziare con:

1 → legacy

3 → P2SH

bc1 → SegWit (oggi i più usati)
Il fatto che inizi con questi numeri indica che si tratta di un indirizzo Bitcoin e non di un'altra criptovaluta. Naturalmente, ogni criptovaluta ha un carattere iniziale specifico che la distingue dalle altre.
La chiave privata, invece, viene generata a partire da un seme unico e irripetibile, assegnato automaticamente da te o dal software che utilizzi. L'unicità garantisce che nessuno possa avere chiavi identiche ed è parte essenziale della sicurezza, impedendo attacchi di forza bruta che potrebbero mettere a rischio i fondi.
Lo schema di questo processo può essere rappresentato più o meno così:
Tornando allo scenario di María e Pedro, quando María vuole inviare bitcoin a Pedro, utilizza la sua chiave privata per firmare ciascuna delle entrate della transazione (cioè la provenienza dei fondi). Questa operazione è eseguita in modo trasparente dal wallet: è compito del portafoglio gestire la firma.
Ad esempio, in Bitcoin si utilizza la crittografia asimmetrica basata su chiave pubblica e privata. In questo modo, i nodi possono validare rapidamente se la transazione è autorizzata dal proprietario. Possono verificare la validità dell'indirizzo di origine, cioè della chiave pubblica, come abbiamo visto. Una volta approvata, la transazione viene ritrasmessa e condivisa da tutti i nodi della rete, registrandola nelle

rispettive blockchain.
Alcuni nodi, inoltre, sono miner. Questi utilizzeranno la transazione insieme a migliaia di altre per risolvere un problema matematico complesso. Così possiamo inviare Bitcoin (e altre criptovalute) in modo completamente sicuro e in pochi secondi a qualsiasi parte del mondo.

Cosa succede se voglio inviare solo una parte di un bitcoin o di un'altra criptovaluta?
Una preoccupazione comune tra chi inizia nel mondo delle criptovalute è come inviare un pagamento a qualcuno, considerando che l'unità di molte criptovalute supera il valore di un dollaro o di un euro.
Il trucco sta nel fatto che molte criptovalute possono essere divise fino a 8 decimali. In altre parole, è possibile inviare quantità molto piccole, fino a centinaia di milioni di frazioni del loro valore.
In Bitcoin, le unità di conto permettono una ampia varietà di micropagamenti. L'unità più piccola, il "satoshi" (in onore del creatore di Bitcoin, l'ignoto Satoshi Nakamoto), è il valore minimo che possiamo avere in Bitcoin.
Tuttavia, in Bitcoin esiste una limitazione alle transazioni minime: non è possibile inviare importi inferiori a 546 satoshi (0,00000546 BTC), conosciuti come transazioni "dust". Questa misura serve a proteggere la rete e prevenire attacchi di tipo "dusting".

Misure simili sono applicate anche ad altre criptovalute, tutte progettate per evitare la congestione della rete e gli attacchi che potrebbero compromettere il corretto funzionamento della blockchain.

Vantaggi delle transazioni con Bitcoin

Velocità

Mentre effettuare una transazione tramite il sistema finanziario tradizionale può richiedere ore o addirittura giorni per l'approvazione o il rifiuto, in Bitcoin tutto è molto più veloce, semplice ed economico. Non servono intermediari che processino e approvino le operazioni: il sistema si basa su una rete di nodi interconnessi che validano le informazioni contenute nelle transazioni, rendendo il processo più rapido, sicuro e affidabile.

Irreversibilità

Una volta effettuata una transazione in Bitcoin e aggiunta alla blockchain, è praticamente impossibile da annullare o modificare. Inoltre, cancellazioni o rimborsi non sono disponibili dopo l'invio della transazione, offrendo un grande vantaggio in diverse aree dell'economia e della finanza.

Sicurezza

Le transazioni in Bitcoin avvengono tramite indirizzi pubblici e chiavi private. Le chiavi private ti danno il diritto di spendere i bitcoin, come un PIN o una password, mentre gli indirizzi pubblici ti permettono di inviare o ricevere bitcoin senza rischi di furto.

Commissioni più economiche.
Le commissioni (fees) pagate ai miner per elaborare una transazione sono davvero basse, soprattutto se confrontate con le percentuali richieste dalle banche o da altri sistemi tradizionali.
Una transazione con criptovalute, indipendentemente dall'importo inviato, può costare solo pochi centesimi, perché le commissioni non si calcolano in base all'ammontare della transazione, ma in base alla dimensione della transazione stessa.