Sommario

[Blockchain: concetti di base 2](#_Toc130216437)

[Come avviene una transazione 4](#_Toc130216438)

[Decentralizzazione 6](#_Toc130216439)

[Tipi di criptovalute 7](#_Toc130216440)

[Wallet: tipi, chiavi, crittografia 8](#_Toc130216441)

[Mining dei blocchi 11](#_Toc130216442)

[Perché fare mining 11](#_Toc130216443)

[Come si realizza il mining 12](#_Toc130216444)

[Validare le transazioni: Proof of Work/Proof of Stake e Game Theory 14](#_Toc130216445)

[Problemi base risolti dalle blockchain 15](#_Toc130216446)

[Riferimenti usati 18](#_Toc130216447)

# Blockchain: concetti di base

* La blockchain è un protocollo software che definisce come trasferire soldi ed asset. Esso è un registro digitale che registra e archivia le informazioni in modo sicuro e trasparente. Si immagini un quaderno digitale a cui possono accedere e aggiornare molte persone allo stesso tempo, ma una volta scritto qualcosa non può essere cancellato o modificato.
* Essa è *decentralizzata*, in quanto non ci sono terze parti coinvolte: banche, cloud, amministratori. L'innovazione di una blockchain è che garantisce la fedeltà e la sicurezza di un record di dati e genera fiducia senza la necessità di una terza parte fidata. Essendo un registro pubblico, garantisce la trasparenza di tutte le transazioni e ne consente la tracciabilità. Se da un lato ciò può consentire una controprova delle informazioni, dall'altro rende difficile la loro falsificazione.
* Le informazioni vengono registrate in modo anonimo e immutabile. Ciò significa che una volta aggiunti al registro, i dati non possono essere rimossi o alterati. Né il fornitore può essere identificato nominativamente.
* I dati sono strutturati a blocchi, ciascuno contenente un set di informazioni. Essi hanno alcune capacità di memoria e, quando riempiti, sono chiuso e collegati al blocco precedente. Tutte le nuove informazioni che seguono il blocco appena aggiunto vengono compilate in un blocco di nuova formazione che verrà aggiunto alla catena una volta riempito.
* Un database di solito struttura i suoi dati in tabelle, mentre una blockchain, come dice il nome stesso, struttura i suoi dati in pezzi (blocchi) che sono collegati tra loro. Questa struttura di dati rende intrinsecamente irreversibile la cronologia dei dati quando è implementata in modo decentralizzato. A ogni blocco della catena viene assegnato un *timestamp* esatto quando viene aggiunto alla catena.
* Per cominciare, i nuovi blocchi sono sempre memorizzati in modo lineare e cronologico. Cioè, vengono sempre aggiunti alla "fine" della blockchain. Dopo che un blocco è stato aggiunto alla fine della blockchain, è estremamente difficile tornare indietro e modificarne il contenuto, a meno che la maggioranza della rete non abbia raggiunto un consenso in tal senso.
* Questo perché ogni blocco contiene il proprio hash, insieme all'hash del blocco precedente e al già citato timestamp. I codici hash sono creati da una funzione matematica che trasforma le informazioni digitali in una stringa di numeri e lettere. Se queste informazioni vengono modificate in qualche modo, anche il codice hash cambia. Inoltre, ogni blocco contiene:
  + Dei dati (data);
  + Un nonce (number used only once), numero generato casualmente quando il blocco è creato
  + Quando viene creato il primo blocco di una catena, un nonce genera l'hash crittografico. I dati contenuti nel blocco sono considerati firmati e legati per sempre al nonce e all'hash, a meno che non vengano estratti.
* Come detto, l’informazione non deve essere alterata; per questo sono anche noti come *distributed ledger technology (DLT)* (in italiano *libro mastro distribuito*), tecnologia alla base delle blockchain.
* In poche parole, un libro mastro distribuito è un database che non ha bisogno di una terza parte per garantire che le transazioni registrate siano valide e oneste. Molti utenti hanno diversi livelli di accesso al database. Le modifiche ai dati vengono registrate automaticamente e non possono essere modificate da un utente senza autorizzazione. In alcuni libri mastri distribuiti, nessuno può apportare modifiche; in altri, le modifiche possono essere apportate, ma sono tracciate e l'utente che le ha apportate è noto.
* La Distributed Ledger Technology (DLT) consente di archiviare le informazioni in modo sicuro e preciso utilizzando la crittografia. L'accesso ai dati può avvenire tramite "chiavi" e firme crittografiche. Una volta memorizzate, le informazioni possono diventare un database immutabile; le regole della rete, scritte nella codifica della programmazione del database, governano il libro mastro.
* Essendo decentralizzati, privati e crittografati, i libri mastri distribuiti sono meno soggetti alla criminalità informatica, in quanto tutte le copie memorizzate nella rete devono essere attaccate simultaneamente perché l'attacco abbia successo. Inoltre, la condivisione e l'aggiornamento peer-to-peer dei record rendono l'intero processo molto più veloce, efficace ed economico.
* Ogni dispositivo di una rete di ledger distribuiti memorizza una copia del libro mastro. Questi dispositivi sono chiamati *nodi*: la rete può avere un numero qualsiasi di nodi. Qualsiasi modifica al libro mastro, come lo spostamento di dati da un blocco all'altro, viene registrata su tutti i nodi. Poiché ogni nodo possiede una copia del libro mastro, ognuno di essi pubblica la propria versione con le ultime transazioni.
* Si noti comunque che di base la decentralizzazione ne è il fattore comune, ma blockchain e DLT differiscono:
  + Le DLT hanno dati concatenati (dunque, non usano blocchi), possono essere criptate, private e con permessi appositi; possono essere immutabili
  + Le blockchain sono memorizzate in blocchi e sono sempre criptate. Sono generalmente pubbliche e senza permessi (permissionless), ma alcune hanno permessi appositi. Sono inoltre sempre immutabili.

## Come avviene una transazione



Riferimento: <https://www.investopedia.com/terms/b/blockchain.asp>

Una transazione in una rete blockchain comporta il trasferimento di beni digitali, come criptovalute o token, da un indirizzo o conto a un altro.

* In primo luogo, ci sono gli utenti, cioè persone che vogliono utilizzare la meccanica della blockchain per effettuare una transazione. Domanda lecita: in un sistema che non ha una struttura centrale, chi lo fa accadere?
* È qui che entrano in gioco i minatori. La blockchain è un sistema privo di fiducia, che consente agli individui di sapere che la loro transazione sarà onorata correttamente senza che vi sia un organismo centrale a supervisionarla. I minatori lo rendono possibile verificando i blocchi di transazione in arrivo, ovvero i lotti di transazioni richieste che attendono (nella mempool, la fase che intercorre tra la richiesta e l'aggiunta alla blockchain) di essere confermate. Se ciò avviene correttamente, si ottiene una ricompensa per i minatori, che è l'incentivo che mantiene in funzione il sistema.
* Paragone del loro utilizzo nel mondo reale:
  + Perché paghiamo le tariffe del gas? Ecco la risposta: compensano l'energia utilizzata nel processo di estrazione delle transazioni e contribuiscono alla ricompensa del blocco per i minatori.
* Infine, ci sono i nodi. Chiunque può essere un nodo. I nodi mantengono l'intero sistema sicuro e protetto convalidando i blocchi di transazioni inviati dai minatori prima che vengano aggiunti alla blockchain. Lo fanno verificando le informazioni in arrivo con la cronologia delle transazioni della blockchain, per assicurarsi che tutto corrisponda. I nodi della rete - sparsi in tutto il pianeta - raggiungono quindi collettivamente un consenso sulla validità delle nuove transazioni, prima di aggiungerle alla blockchain.

Ecco una spiegazione semplificata di come avviene una transazione in una blockchain:

1. L'utente avvia la transazione creando una firma digitale utilizzando la propria chiave privata. La firma dimostra che l'utente ha il diritto di inviare i beni.
2. La transazione viene trasmessa alla rete di nodi o computer che eseguono il software della blockchain. Ogni nodo riceve la transazione e la aggiunge a un pool di transazioni non confermate.
3. I nodi della rete convalidano la transazione per assicurarsi che il mittente abbia fondi sufficienti per completare la transazione e che questa sia conforme alle regole del protocollo blockchain.
4. Una volta che un numero sufficiente di nodi ha convalidato la transazione, questa viene aggiunta a un nuovo blocco di transazioni, insieme ad altre transazioni convalidate di recente.
5. Il blocco di transazioni viene aggiunto alla blockchain in un processo chiamato mining. L'estrazione comporta la risoluzione di complesse equazioni matematiche per creare un nuovo blocco, il che richiede una grande potenza di calcolo.
6. Una volta aggiunto il nuovo blocco alla blockchain, la transazione viene considerata confermata e i beni vengono trasferiti dall'indirizzo del mittente a quello del destinatario. La transazione è ora registrata in modo permanente sul libro mastro della blockchain, che può essere visualizzato e verificato da chiunque abbia accesso alla rete.
7. Infine, l'utente può controllare lo stato della sua transazione utilizzando il *blockchain explorer*, uno strumento che consente di visualizzare i dettagli della transazione e il suo avanzamento nella rete blockchain. Essendo decentralizzate, questo permette a tutti di vedere le transazioni che avvengono in diretta.
   1. Questo strumento presenta la blockchain in una maniera user-friendly, spesso tramite un’interfaccia web che permetta agli utenti di cercare e filtrare le informazioni secondo vari criteri. In particolare, si possono cercare
      1. Le singole transazioni (inserendo la hash, indirizzo, numero di blocco)
      2. I singoli indirizzi
      3. I dettagli sui blocchi
      4. Le statistiche sulla rete
      5. Grafici sulle performance

In generale, il processo di una transazione in una blockchain prevede la creazione di una firma digitale, la trasmissione della transazione alla rete, la convalida della transazione, l'aggiunta a un nuovo blocco, il mining del blocco, la conferma della transazione e la registrazione permanente sulla blockchain.

## Decentralizzazione

* La blockchain consente di distribuire i dati contenuti nel database tra diversi nodi della rete in varie località. Questo non solo crea *ridondanza*, ma mantiene anche la fedeltà dei dati memorizzati: se qualcuno tenta di alterare un record in un'istanza del database, gli altri nodi non verrebbero alterati, impedendo così a un malintenzionato di farlo. Se un utente manomette il registro delle transazioni di Bitcoin, tutti gli altri nodi fanno un *riferimento incrociato* e individuano facilmente il nodo con le informazioni errate. Questo sistema aiuta a stabilire un ordine preciso e trasparente degli eventi. In questo modo, nessun singolo nodo della rete può alterare le informazioni in essa contenute.
* Ogni nodo ha la propria copia della blockchain e la rete deve approvare algoritmicamente ogni nuovo blocco estratto affinché la catena sia aggiornata, affidabile e verificata. Poiché le blockchain sono trasparenti, ogni azione nel libro mastro può essere facilmente controllata e visualizzata, creando una sicurezza intrinseca della blockchain. A ogni partecipante viene assegnato un numero di identificazione alfanumerico unico che indica le sue transazioni.
* La combinazione di informazioni pubbliche con un sistema di controlli e bilanciamenti aiuta la blockchain a mantenere l'integrità e a creare fiducia tra gli utenti. In sostanza, le blockchain possono essere considerate come la scalabilità della fiducia attraverso la tecnologia. Per questo motivo, le informazioni e la storia (ad esempio delle transazioni di una criptovaluta) sono *irreversibili*. Un record di questo tipo potrebbe essere un elenco di transazioni (come nel caso di una criptovaluta), ma è anche possibile che una blockchain contenga una serie di altre informazioni come contratti legali, identificazioni statali o l'inventario dei prodotti di un'azienda.
* Poniamo alcuni concetti base sulla decentralizzazione:
  + Rete distribuita: Una rete blockchain è costituita da molti nodi o computer che lavorano insieme per convalidare e registrare le transazioni sul libro mastro della blockchain. Ogni nodo mantiene una copia del libro mastro, che viene aggiornato in tempo reale quando vengono aggiunte nuove transazioni. Poiché il libro mastro è distribuito tra molti nodi, non esiste un singolo punto di errore o di controllo.
  + Meccanismo di consenso: Per garantire che tutti i nodi della rete concordino sullo stato del libro mastro, le reti blockchain utilizzano un meccanismo di consenso. Si tratta di un insieme di regole che disciplinano il modo in cui le nuove transazioni vengono convalidate e aggiunte alla blockchain. Ad esempio, la blockchain Bitcoin utilizza un meccanismo di consenso proof-of-work, in cui i nodi competono per risolvere complessi puzzle matematici per aggiungere nuovi blocchi alla catena.
  + Sistema senza fiducia (trustless system): In una rete blockchain decentralizzata, le transazioni vengono convalidate e registrate senza la necessità di un intermediario fidato, come una banca o un governo. La rete si basa invece sulla crittografia e sul consenso per garantire la sicurezza e l'affidabilità delle transazioni. Ciò significa che chiunque può partecipare alla rete senza doversi fidare di un'autorità centrale.
  + Aperta e trasparente: Le blockchain decentralizzate sono spesso aperte e trasparenti, il che significa che chiunque può visualizzare e verificare le transazioni e i dati registrati sulla blockchain. Ciò garantisce un elevato grado di trasparenza e responsabilità, particolarmente importante in settori come la finanza, la gestione della catena di approvvigionamento e le votazioni.
  + Sfide di scalabilità: Una delle sfide della decentralizzazione nella blockchain è la scalabilità. Quando un numero maggiore di utenti si unisce alla rete e vengono aggiunte più transazioni, la rete può diventare più lenta e più costosa da gestire. Questo ha portato allo sviluppo di nuove tecnologie blockchain, come lo sharding e le sidechain, che mirano a migliorare la scalabilità delle reti decentralizzate.

## Tipi di criptovalute

Le criptovalute sono beni digitali creati e scambiati con tecniche crittografiche, costruite sul sistema blockchain. Listiamo i tipi principali:

* Il Bitcoin, la prima e più nota criptovaluta, è stato creato nel 2009 da una persona o un gruppo anonimo noto come Satoshi Nakamoto. Utilizza una blockchain per registrare tutte le transazioni e i nuovi bitcoin vengono creati attraverso un processo chiamato mining. Il mining consiste nel risolvere complessi problemi matematici per verificare le transazioni e aggiungerle alla blockchain.
  + Una delle caratteristiche interessanti di Bitcoin è la sua limitata fornitura di unità di valuta. Esistono solo 21 milioni di bitcoin, e finora ne sono stati creati circa 18,5 milioni. La quantità di bitcoin che viene creata in ogni blocco della blockchain viene ridotta a metà circa ogni 4 anni in un processo noto come "halving". Questo significa che la produzione di bitcoin si ridurrà gradualmente fino a quando non si raggiungerà la quantità massima di 21 milioni.
  + Per contro, l'infrastruttura blockchain di Bitcoin inizia a rallentare una volta superata la velocità di sette transazioni al secondo.
* Ethereum è una piattaforma decentralizzata basata su blockchain, che permette agli utenti di creare e gestire contratti intelligenti e applicazioni decentralizzate (DApps). La sua criptovaluta nativa è l'Ethereum (ETH), che viene utilizzata per pagare le transazioni sulla rete Ethereum.
  + Rispetto ad altre valute, Ethereum si distingue principalmente per la sua funzionalità di contratti intelligenti, che consentono di eseguire automaticamente accordi e transazioni senza l'intervento di intermediari. Questo significa che le applicazioni costruite sulla piattaforma Ethereum possono essere programmate per eseguire operazioni complesse, come ad esempio la gestione di contratti finanziari, senza la necessità di un intermediario di fiducia.
  + Un'altra differenza significativa è la sua capacità di supportare token personalizzati e DApps, che possono essere sviluppati sulla piattaforma Ethereum. Ciò significa che gli sviluppatori possono creare nuove applicazioni decentralizzate che utilizzano la tecnologia di Ethereum come base, piuttosto che dover creare una propria blockchain da zero.
  + Inoltre, Ethereum è in grado di elaborare transazioni più velocemente rispetto a Bitcoin, poiché utilizza un algoritmo di consenso diverso chiamato Proof of Stake (PoS). Questo algoritmo richiede meno energia rispetto al Proof of Work (PoW) utilizzato da Bitcoin e altre valute, il che significa che la rete Ethereum può elaborare più transazioni in meno tempo.
* Ripple è una piattaforma di pagamenti globale basata sulla tecnologia blockchain, che utilizza il proprio token nativo XRP per facilitare le transazioni finanziarie transfrontaliere. La piattaforma Ripple consente ai pagamenti internazionali di essere elaborati in modo rapido e conveniente, senza la necessità di intermediari tradizionali come banche corrispondenti.
  + Rispetto ad altre valute, Ripple si distingue per il suo focus sulle transazioni finanziarie transfrontaliere. La piattaforma è progettata per fornire una soluzione efficiente ai problemi di liquidità transfrontaliera, che spesso impediscono la rapida elaborazione dei pagamenti internazionali.
  + Inoltre, Ripple utilizza un protocollo di consenso unico chiamato Ripple Protocol Consensus Algorithm (RPCA), che consente di validare le transazioni in modo più efficiente rispetto al Proof of Work (PoW) utilizzato da Bitcoin. Ciò significa che la piattaforma Ripple può elaborare un grande volume di transazioni in modo rapido ed efficiente.
  + Infine, Ripple ha stretto relazioni con le banche e le istituzioni finanziarie, il che lo rende un'opzione più attraente per le istituzioni finanziarie rispetto ad altre criptovalute che possono essere viste come più rischiose.

## Wallet: tipi, chiavi, crittografia

Un portafoglio blockchain è un portafoglio di criptovalute che consente agli utenti di gestire diversi tipi di criptovalute, ad esempio Bitcoin o Ethereum. Un portafoglio blockchain aiuta a scambiare facilmente i fondi. Le transazioni sono sicure, poiché sono firmate crittograficamente. Il portafoglio è accessibile dai dispositivi web, compresi quelli mobili, e la privacy e l'identità dell'utente sono mantenute. l wallet, anche se si chiama portafoglio, in realtà è un portachiavi, perché non contiene realmente gli asset, ma conserva solo le chiavi per accedervi.

* In primo luogo, occorre scaricare il portafoglio blockchain e creare un account. Dopodiché si riceve una coppia di chiavi, composta da una chiave pubblica e da una chiave privata. Queste chiavi vi aiuteranno a ricevere e trasferire fondi dal vostro conto.
  + La *chiave pubblica* viene fornita per inviare messaggi e ricevere pagamenti. Ogni volta che qualcuno desidera inviarvi dei bitcoin, o qualsiasi altra criptovaluta, dovrà includere la chiave pubblica e la sua chiave privata per completare la transazione. Essa è un indirizzo alfanumerico formato da 32 caratteri
  + La *chiave privata* è per un portafoglio di criptovalute simile al PIN del bancomat o al TAN dell'Online Banking per un conto bancario. Ogni portafoglio ha una o più chiavi private uniche. È nota solo al proprietario del portafoglio e viene utilizzata per dimostrare che possiede legittimamente il conto e i fondi contenuti e può inviare transazioni. Ogni transazione crittografica inviata è firmata con la chiave privata del portafoglio, che tuttavia non viene rivelata a terzi.
* La *moltiplicazione della curva ellittica (elliptic curve multiplication)* è un'operazione matematica fondamentale utilizzata per la creazione di chiavi pubbliche e private per l'utilizzo della blockchain.

Viene utilizzata per generare queste coppie di chiavi pubbliche e private. Il processo consiste nel partire da un punto scelto su una curva ellittica e nel moltiplicarlo per un grande numero casuale (la chiave privata) per ottenere un nuovo punto della curva (la chiave pubblica). Questo processo è matematicamente reversibile: la chiave privata può essere utilizzata per generare la chiave pubblica, ma la chiave pubblica non può essere utilizzata per determinare la chiave privata.

* La sicurezza della crittografia a curva ellittica risiede nel fatto che è estremamente difficile invertire il processo e calcolare la chiave privata dalla chiave pubblica. Questo rende praticamente impossibile per chiunque rubare fondi da un portafoglio senza avere accesso alla chiave privata.
* Se un utente dovesse perdere (e/o dimenticare) la chiave privata del suo portafoglio, non potrebbe più accedere, gestire o inviare i fondi contenuti nel portafoglio. In breve, i fondi andrebbero irrimediabilmente persi. Per evitare che ciò accada, nei portafogli di criptovalute è presente un meccanismo di backup chiamato frase segreta (talvolta indicata anche come frase mnemonica, seme di backup, frase di recupero).
* La *frase segreta* è un insieme di 12-24 parole che contiene tutte le informazioni necessarie per recuperare e accedere a tutti i fondi di un portafoglio crittografico. Può essere utilizzata per ricavare la chiave privata del portafoglio, poiché la frase segreta è una rappresentazione del numero casuale della chiave privata. I fornitori di portafogli indicheranno agli utenti di annotare la frase segreta generata su un pezzo di carta e di conservarla in modo sicuro, fuori dalla portata di terzi.
* Ciascun wallet ha un suo indirizzo (*wallet address*). L'indirizzo del portafoglio è matematicamente derivato dalla chiave pubblica del portafoglio attraverso una funzione unidirezionale chiamata "hashing". L'indirizzo del portafoglio è una rappresentazione più breve della parte finale della chiave pubblica e di solito ha una lunghezza di 160 bit. L'indirizzo del portafoglio e la chiave pubblica non sono la stessa cosa, poiché l'indirizzo del portafoglio è la parte finale della chiave pubblica.
* Gli indirizzi sono *pseudonimi* dato che non si sa esattamente a quale entità fisica o meno possano corrispondere dato il numero di caratteri. Non è completamente anonimo, ma non si può affermare che sia identificato nello specifico da una certa persona.

Ci sono due tipi principali di wallet:

* Gli *hot wallet* vengono utilizzati con l'aiuto di Internet e sono considerati di facile utilizzo. Il problema principale è la sicurezza. A causa della connettività a Internet, sono più inclini al rischio di hacking. Per questo motivo gli esperti non consigliano di tenere una grande somma in un portafoglio hot. Ve ne sono di vario tipo:
  + Mobile wallet - I portafogli mobili sono piuttosto comodi per gli utenti, poiché l'interfaccia è molto facile da usare. È possibile installare facilmente un portafoglio mobile sul proprio smartphone. Gli investitori tendono a utilizzare questo portafoglio per effettuare le transazioni quotidiane con l'aiuto del codice QR che ricevono. I portafogli mobili possono essere molto vantaggiosi per molti investitori. Possono verificarsi problemi come virus e infezioni da malware.
  + Desktop wallet - Questi portafogli possono essere installati sul desktop come software. Possono essere un'ottima fonte per conservare le criptovalute. Assicuratevi di avere un antivirus sul vostro desktop, in modo da ridurre il rischio di hacking e mantenere la sicurezza. Hanno un'interfaccia utente molto amichevole e forniscono una privacy di prim'ordine. Inoltre, sono considerati il terzo portafoglio più sicuro per l'archiviazione di criptovalute.
  + Web wallet - Questi portafogli sono accessibili solo attraverso un browser web. Possono essere utilizzati in modalità hosted o non-hosted. Gli esperti raccomandano l'uso di un metodo non ospitato perché consente di mantenere il controllo sulle criptovalute. Il fatto che si possa accedere solo attraverso un browser web lo rende molto esposto agli attacchi. È considerato il portafoglio meno sicuro, quindi vi consigliamo di non investire grandi somme attraverso un portafoglio web. È perfetto se si vogliono fare solo piccoli investimenti o transazioni veloci.
* I *cold wallet* sono considerati un'opzione altamente sicura per conservare le criptovalute. Uno degli aspetti migliori di questi tipi di portafogli è che non sono collegati a Internet. Si collegano a internet solo quando si effettuano le transazioni. Molti investitori in criptovalute preferiscono utilizzare i portafogli a freddo. Non solo perché sono sicuri, ma anche facili da usare. La cosa migliore è che sono dotati di assistenza clienti. Essi comprendono:
  + Hardware wallet - Un portafoglio hardware utilizza dispositivi hardware per memorizzare in modo sicuro le chiavi private. È considerato uno dei portafogli migliori e sicuri per conservare le chiavi lontano dalla portata degli hacker. In genere, il costo si aggira tra i 70 e i 150 dollari. Può sembrare un po' costoso, ma ne vale la pena perché offre un'elevata sicurezza per le chiavi. Per quanto riguarda l'aspetto, si tratta di un dispositivo USB composto da pulsanti laterali e da uno schermo OLED. L'interfaccia è molto migliore rispetto a quella del portafoglio cartaceo. Ma se siete principianti, non scegliete un portafoglio hardware. Potrebbe non essere piacevole per gli occhi.
  + Paper wallet - I portafogli di carta sono simili ai portafogli hardware. Ma conservano le chiavi private su pezzi di carta invece che su un dispositivo hardware come l'USB. Sono anche molto sicuri e per gli hacker è molto difficile attaccarli. I portafogli cartacei erano piuttosto famosi nel mercato delle criptovalute fino all'arrivo dei portafogli hardware. I portafogli hardware avevano molte caratteristiche migliori rispetto a quelli cartacei. È proprio questo che ha spinto molti investitori a smettere di usare i portafogli cartacei e a optare per un'opzione migliore.

## Mining dei blocchi

* Il processo di mining permette di creare nuovi blocchi sulla catena. In una blockchain ogni blocco ha un nonce e un hash unici, ma fa anche riferimento all'hash del blocco precedente nella catena, quindi estrarre un blocco non è facile, soprattutto nelle catene di grandi dimensioni. L'obiettivo del processo di mining nel contesto della blockchain è aggiungere nuove transazioni al registro della blockchain e convalidarle. Questo obiettivo viene raggiunto attraverso un processo chiamato *consenso*, che prevede la risoluzione di complessi puzzle matematici utilizzando la potenza di calcolo.
* I minatori (miners) utilizzano un software speciale per risolvere il problema matematico incredibilmente complesso di trovare un nonce che generi un hash accettato. Poiché il nonce è di soli 32 bit e l'hash di 256, ci sono circa quattro miliardi di possibili combinazioni nonce-hash che devono essere estratte prima di trovare quella giusta. Quando ciò accade, si dice che i minatori hanno trovato il "nonce d'oro" e il loro blocco viene aggiunto alla catena.
* Per modificare un blocco precedente nella catena è necessario estrarre nuovamente non solo il blocco con la modifica, ma anche tutti i blocchi successivi. Ecco perché è estremamente difficile manipolare la tecnologia blockchain. Si pensi alla "sicurezza in matematica", poiché trovare i nonce d'oro richiede un'enorme quantità di tempo e di potenza di calcolo.
* Quando un blocco viene estratto con successo, la modifica viene accettata da tutti i nodi della rete e il miner viene ricompensato finanziariamente. Il primo minatore che risolve il puzzle e aggiunge un nuovo blocco alla blockchain viene ricompensato con un blocco di criptovaluta di nuovo conio. Questo incentiva i minatori a contribuire con la loro potenza di calcolo alla rete e aiuta a distribuire equamente la criptovaluta tra i partecipanti alla rete.

### Perché fare mining

Il processo di mining può diventare molto complesso e un normale desktop o PC non è sufficiente. Per questo motivo, è necessario un set unico di hardware e software che funzioni bene per l'utente. È utile avere un set personalizzato specifico per l'estrazione di determinati blocchi.

Questo succede in particolare per tre motivazioni principali:

1. *Meccanismo di consenso proof-of-work*: Molte reti blockchain, come Bitcoin, utilizzano un meccanismo di consenso proof-of-work per convalidare le transazioni e aggiungere nuovi blocchi alla blockchain. Ciò richiede la risoluzione di un complesso puzzle matematico, noto come funzione hash, utilizzando la potenza di calcolo. Il primo miner che risolve il puzzle viene ricompensato con un blocco di criptovaluta di nuovo conio. La difficoltà del rompicapo aumenta nel tempo con l'ingresso di altri minatori nella rete, che richiedono maggiore potenza di calcolo per essere risolti.
2. *Competizione tra minatori*: L'estrazione di blockchain è un processo competitivo, con i minatori che competono tra loro per risolvere il puzzle ed essere i primi ad aggiungere un nuovo blocco alla catena. Questa competizione crea una corsa alla potenza di calcolo, in quanto i minatori cercano di superarsi l'un l'altro con hardware più potente per aumentare le loro possibilità di vincere la ricompensa.
3. *Requisiti di elaborazione e archiviazione*: Oltre alla potenza di calcolo necessaria per risolvere il puzzle, il mining per la blockchain richiede anche una quantità significativa di capacità di elaborazione e di archiviazione per convalidare e registrare le transazioni. Ciò richiede hardware potente, come schede grafiche di fascia alta e piattaforme di mining specializzate, per gestire il carico di lavoro in modo efficiente.

Il processo di estrazione può essere suddiviso in tre categorie:

1. Estrazione individuale

Quando l'attività di mining viene svolta da un individuo, è necessaria la registrazione dell'utente come minatore. Non appena avviene una transazione, a tutti i singoli utenti della rete blockchain viene sottoposto un problema matematico da risolvere. Il primo che lo risolve viene premiato.

Una volta trovata la soluzione, tutti gli altri minatori della rete blockchain convalideranno il valore decifrato e lo aggiungeranno alla blockchain. In questo modo, la transazione viene verificata.

1. Mining in pool

Nel pool mining, un gruppo di utenti lavora insieme per approvare la transazione. A volte, la complessità dei dati crittografati nei blocchi rende difficile per un utente decifrare i dati codificati da solo. Pertanto, un gruppo di minatori lavora in squadra per risolvere il problema. Dopo la convalida del risultato, la ricompensa viene divisa tra tutti gli utenti.

1. Mining in cloud

Il cloud mining elimina la necessità di hardware e software. È un metodo senza problemi per estrarre i blocchi. Con il cloud mining, la gestione di tutti i macchinari, la tempistica degli ordini o la vendita dei profitti non sono più una preoccupazione costante.

### Come si realizza il mining

I minatori utilizzano un software specializzato per partecipare al processo di estrazione e convalidare le transazioni sulla blockchain. Il software è progettato per funzionare con la rete blockchain specifica su cui viene effettuato il mining e comprende in genere i seguenti componenti:

* *Client di mining*: Il client di mining è l'applicazione software principale utilizzata dai minatori per partecipare al processo di mining. Collega l'hardware del miner alla rete blockchain e comunica con gli altri nodi della rete per convalidare le transazioni e aggiungere nuovi blocchi alla catena.
* *Portafoglio*: Un portafoglio è utilizzato per memorizzare la criptovaluta guadagnata dal miner come ricompensa per la convalida delle transazioni e l'aggiunta di nuovi blocchi alla blockchain. Il portafoglio è solitamente incluso nel software di mining e può essere utilizzato anche per inviare e ricevere criptovalute.
* *Software di pool di mining*: Alcuni minatori scelgono di unirsi a pool di mining, che sono gruppi di minatori che uniscono la loro potenza di calcolo per aumentare le possibilità di guadagnare una ricompensa. Il software del pool di mining viene utilizzato per gestire il pool e distribuire le ricompense tra i minatori partecipanti.
* *Driver hardware*: I minatori utilizzano hardware specializzato, come ASIC (Application-Specific Integrated Circuits), GPU (Graphics Processing Units) o CPU (Central Processing Units), per risolvere i rompicapo matematici richiesti dal mining. Il software di mining deve essere compatibile con l'hardware specifico utilizzato dal miner e richiede l'installazione dei driver appropriati sul sistema.

Approfondiamo ad esempio gli ASIC, sviluppati a partire dal 2012. I miner ASIC sono progettati specificamente per fornire le migliori prestazioni possibili alle criptovalute cui sono destinati. Sono progettati esclusivamente per l'estrazione di criptovalute; a parte questo, la loro potenza è di scarsa utilità.

* Il processo di produzione degli ASIC è altamente specializzato e prevede una serie di fasi complesse, tra cui la progettazione, la fabbricazione e il collaudo. Il processo di progettazione prevede la creazione di un layout di circuito personalizzato e la sua ottimizzazione per ottenere le massime prestazioni ed efficienza. Una volta finalizzato il progetto, il circuito viene fabbricato utilizzando tecniche di produzione avanzate come la litografia, l'incisione e la deposizione.
* Dopo la produzione, gli ASIC vengono testati per garantire che soddisfino le specifiche richieste per il mining di criptovalute. Questo processo di verifica prevede che gli ASIC vengano sottoposti a una serie di test rigorosi per garantire che possano eseguire i calcoli richiesti in modo accurato ed efficiente. Le parti tipiche che compongono una postazione da ASIC mining sono il software per il mining, il chip ASIC, una fonte di alimentazione e le ventole per raffreddare il sistema.
* Nel complesso, gli ASIC sono un componente critico dell'ecosistema di mining di criptovalute e sono essenziali per i minatori che vogliono competere in un ambiente di mining altamente competitivo. Il loro design specializzato e l'elevata potenza di elaborazione li rendono uno strumento prezioso per il mining di criptovalute in modo efficiente e redditizio. Di fatto, sono molto costosi e hanno un’elevata potenza di calcolo che si traduce in un alto dispendio e consumo di energia.

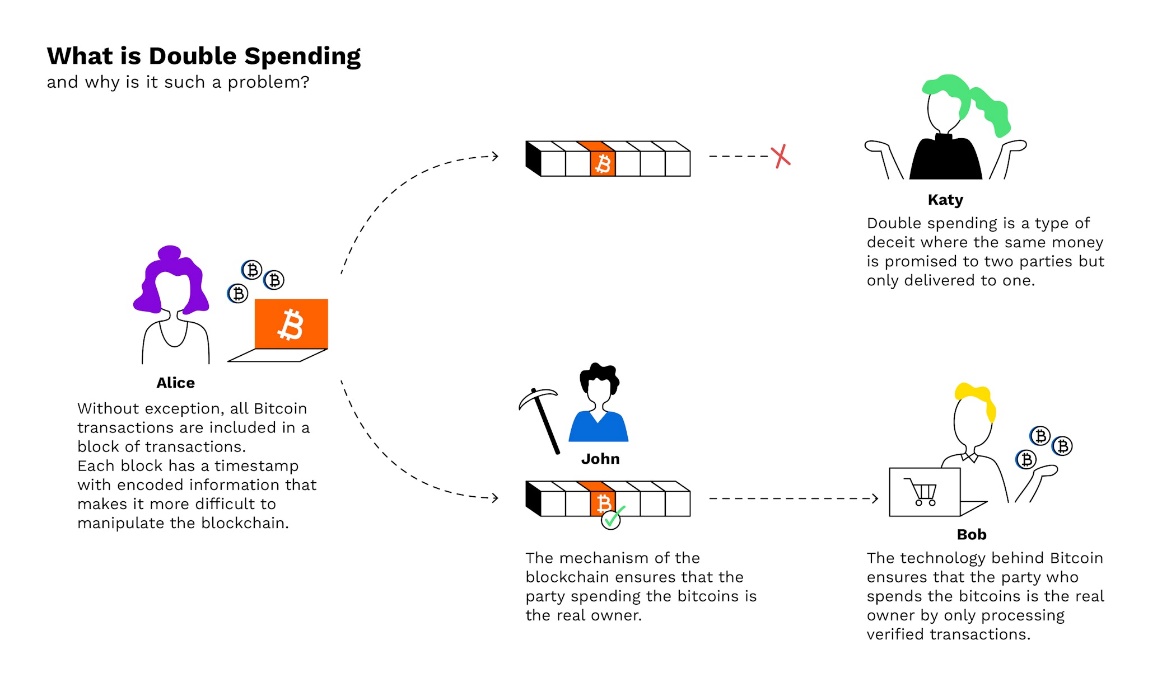
Qualche esempio di dispositivo:

* <https://www.hola-cripto.com/corso-criptovalute/cosa-e-asic-mining-e-come-funziona/>
* <https://academy.bit2me.com/it/que-son-mineros-asic/>

## Validare le transazioni: Proof of Work/Proof of Stake e Game Theory

## Problemi base risolti dalle blockchain

* Per i soldi, si vuole evitare il “*double spend problem*” (detto anche *problema della doppia spesa*), quindi occorre fare in modo che i soldi vengano spediti una volta sola senza essere copiati più volte come accade per altri file. Come detto, si riferisce alla possibilità che un utente spenda due volte la stessa unità di criptovaluta, creando due transazioni diverse che utilizzano la stessa unità di criptovaluta. Questo problema è dovuto al fatto che, se fosse permesso, porterebbe a frodi e alla svalutazione della criptovaluta.



Riferimento: <https://www.bitpanda.com/academy/en/lessons/what-is-double-spending-and-why-is-it-such-a-problem/>

* + La soluzione al problema della doppia spesa si ottiene attraverso l'uso di un *sistema di registro distribuito* (*distributed ledger system*), gestito da una rete di nodi o computer che convalidano e registrano collettivamente le transazioni. Questo sistema di libro mastro è progettato per prevenire la possibilità di doppia spesa garantendo che ogni transazione sia convalidata e confermata da più nodi della rete.
  + Quando viene avviata una transazione, questa viene trasmessa all'intera rete e ogni nodo della rete la convalida in modo indipendente per assicurarsi che il mittente abbia fondi sufficienti per completare la transazione. Una volta che un numero sufficiente di nodi ha convalidato la transazione, questa viene aggiunta alla blockchain, che è un registro permanente e a prova di manomissione di tutte le transazioni avvenute sulla rete.
  + Una volta che una transazione è confermata e registrata sulla blockchain, diventa praticamente impossibile spendere due volte la stessa unità di criptovaluta, perché qualsiasi tentativo di farlo richiederebbe la modifica della blockchain da parte di un aggressore, che verrebbe immediatamente rilevato dalla rete e rifiutato.
* Altro problema è il *Byzantine Generals Agreement problem* (oppure *Byzantine fault tolerance*), è un problema fondamentale nei sistemi di calcolo distribuito, dove un gruppo di nodi o computer deve lavorare insieme per raggiungere un obiettivo comune. In questo caso, questo problema riguarda il raggiungimento di consenso comune da parte di tutti i nodi della rete.



Riferimento: <https://river.com/learn/what-is-the-byzantine-generals-problem/>

* Esso prende il nome da un ipotetico scenario in cui un gruppo di generali bizantini deve coordinare i propri piani di attacco per conquistare una città. Il problema è che alcuni dei generali possono essere dei traditori che cercano di interrompere la comunicazione tra gli altri generali, rendendo impossibile raggiungere un consenso su quando e come attaccare la città.
  + Il problema sorge quando alcuni dei nodi della rete sono difettosi o compromessi e possono inviare messaggi contraddittori o cercare di sabotare il funzionamento della rete. Questo può portare a un'interruzione della capacità della rete di raggiungere un consenso o di prendere decisioni, il che può essere disastroso in sistemi mission-critical come le transazioni finanziarie, la gestione della catena di approvvigionamento o le operazioni militari.
  + La tecnologia blockchain risolve il problema dell'accordo generale bizantino utilizzando un protocollo di consenso distribuito che consente alla rete di raggiungere un consenso anche se alcuni nodi sono difettosi o maligni.
  + In una rete blockchain, ogni nodo mantiene una copia del libro mastro della blockchain e convalida le nuove transazioni in base a un insieme di regole o protocolli predefiniti. Quando viene proposta una nuova transazione, questa viene trasmessa all'intera rete e ogni nodo la convalida in modo indipendente prima di aggiungerla alla propria copia della blockchain.
  + Per prevenire la possibilità di un doppio attacco, la blockchain utilizza un meccanismo di consenso, come la *proof-of-work* o la *proof-of-stake*, per garantire che ogni nuovo blocco di transazioni sia convalidato e approvato dalla maggioranza dei nodi della rete. In questo modo si garantisce che, anche se alcuni nodi sono difettosi o maligni, la maggioranza della rete possa comunque raggiungere un consenso sullo stato del libro mastro.
  + Inoltre, l'uso della crittografia nella tecnologia blockchain garantisce che le transazioni e il funzionamento della rete siano sicuri e a prova di manomissione. Qualsiasi tentativo di modificare la blockchain richiederebbe che l'aggressore controlli la maggior parte della potenza di calcolo della rete, cosa virtualmente impossibile in una rete decentralizzata con un gran numero di nodi.
  + Pertanto, utilizzando un protocollo di consenso distribuito e misure di sicurezza crittografiche, la tecnologia blockchain fornisce una soluzione al problema dell'accordo generale bizantino, consentendo una comunicazione e un processo decisionale sicuri e affidabili nei sistemi decentralizzati.

# Riferimenti usati

* Corso Blockchain Theory 101 Udemy: <https://www.udemy.com/course/blockchain-theory-101>
* Investopedia: <https://www.investopedia.com/>
* BitPanda: <https://www.bitpanda.com/>
* Intellipaat: <https://intellipaat.com/>
* HolaCripto: <https://www.hola-cripto.com/>
* Simplilearn: <https://www.simplilearn.com/>
* Blocktrade: <https://blocktrade.com/>