Sommario

[Blockchain: concetti di base 2](#_Toc130461021)

[Problemi di sicurezza nelle blockchain 4](#_Toc130461022)

[Come avviene una transazione 8](#_Toc130461023)

[Tipi di transazioni 10](#_Toc130461024)

[Decentralizzazione 10](#_Toc130461025)

[Tipi di criptovalute 12](#_Toc130461026)

[Wallet: tipi, chiavi, crittografia a chiave pubblica 14](#_Toc130461027)

[Crittografia nelle blockchain 16](#_Toc130461028)

[Mining dei blocchi 19](#_Toc130461029)

[Perché fare mining 20](#_Toc130461030)

[Come si realizza il mining 21](#_Toc130461031)

[Considerazioni sul mining 22](#_Toc130461032)

[Algoritmi di consenso 22](#_Toc130461033)

[Proof of Work 22](#_Toc130461034)

[Proof of Stake 26](#_Toc130461035)

[Alcune tipologie di consenso 29](#_Toc130461036)

[Tipi di blockchain 36](#_Toc130461037)

[Sidechain 39](#_Toc130461038)

[Scalabilità nelle blockchain 42](#_Toc130461039)

[Directed Acyclic Graphs (DAG) 44](#_Toc130461040)

[Riferimenti usati 47](#_Toc130461041)

# 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. Il sistema è definito *peer-to-peer (p2p),* in quanto trasferisce valore tra due utenti senza un intermediario
* 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.
* Esistono le cosiddette fork, cioè le modifiche al protocollo/regole di base delle blockchain. La rete è un software open source e il codice è liberamente disponibile. Ciò significa che chiunque può proporre miglioramenti e modificare il codice. La possibilità di sperimentare sul software open source è una parte fondamentale delle criptovalute e facilita anche gli aggiornamenti del software della blockchain.
  + In ogni momento, migliaia di minatori sono in competizione per creare un nuovo blocco. Con un'attività di mining così intensa, a volte due o più minatori creano un nuovo blocco nello stesso momento. Quando ciò accade, si crea un *fork accidentale*. Il problema si risolve quando vengono aggiunti nuovi blocchi a una delle catene. In questo caso, la rete continua a lavorare sulla catena più lunga e abbandona quella più corta.
  + Quando si crea una biforcazione intenzionale, la rete non si riconverte su una singola catena. Questo tipo di fork viene utilizzato dagli sviluppatori di blockchain per implementare modifiche al protocollo. Ad esempio, gli sviluppatori possono utilizzare una fork intenzionale per aumentare le dimensioni dei blocchi, ridurre il tempo di blocco o persino implementare un algoritmo di consenso completamente nuovo.
    - In questi fork distinguiamo gli *hard fork*, in cui i membri della comunità (utenti e minatori) devono prendere una decisione. Possono aggiornare il loro nodo e passare alla nuova catena forzata, oppure possono continuare a utilizzare il vecchio software. In ogni caso, possiedono criptovalute su entrambe le catene: hanno monete sulla catena precedente e possono rivendicare le criptovalute del nuovo protocollo sulla nuova catena.
      * Normalmente sono forzati (hard) ad aggiornare, in quanto i nodi che non si adeguano alle nuove regole di consenso non possono più partecipare al meccanismo di consenso presente.
    - A differenza degli hard fork, le modifiche implementate dai *soft fork* rendono le catene compatibili con il futuro. Per essere compatibili con il futuro, i blocchi creati secondo le nuove regole devono essere validi anche secondo le vecchie regole (ma non viceversa). Per questo motivo, un soft fork non richiede l'aggiornamento dei nodi. Possono continuare a eseguire la vecchia versione del software e partecipare alla rete aggiornata come validatori di transazioni.
      * Le soft fork possono essere attivate dagli utenti (UASF, ovvero user activated soft fork) o dai miner (MASF, ovvero miner activated soft fork).

## Problemi di sicurezza nelle blockchain

Un problema rilevante è il double spending 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.

Un altro problema rilevante è il selfish mining, tecnica di attacco alla sicurezza delle blockchain basate sul Proof of Work (PoW). In pratica, il selfish mining consente a un miner di ottenere una maggiore ricompensa rispetto agli altri miner senza dover effettivamente eseguire un lavoro maggiore.

* Il selfish mining funziona in modo simile ad un attacco di double-spending. In pratica, il miner che utilizza il selfish mining raccoglie informazioni sulle transazioni e sullo stato corrente della blockchain, e cerca di costruire un blocco in segreto, formandosi un branch segreto.

Immagine che contiene testo, orologio, manometro

Descrizione generata automaticamente

Riferimento: <https://decentralizedthoughts.github.io/2020-02-26-selfish-mining/>

* Una volta che il miner ha costruito un blocco, lo tiene segreto invece di condividerlo con la rete. In questo modo, il miner può continuare a lavorare sul blocco successivo, aumentando le sue possibilità di risolvere il puzzle crittografico e di aggiungere il nuovo blocco alla blockchain. In pratica, continua ad estendere il suo branch segreto finché la catena pubblica non è ad un passo indietro. Allora viene pubblicato; essendo più lungo della catena principale, viene considerata come tale e i blocchi degli altri utenti vengono ignorati. Deve però essere il primo a pubblicare il blocco quando la catena è più lunga, altrimenti la strategia non funziona.
* Soluzioni possibili: cercare di assegnare in maniera casuale minatori ai rami della blockchain quando avviene un branch oppure settare limiti di soglia alle pool di mining della rete che preverrebbero ai selfish minera di avere vantaggi significativi sulla rete.

L'attacco del 51% (51 percent attack) è un attacco informatico in cui un attaccante controlla più della metà della potenza di calcolo della rete. In pratica, ciò significa che l'attaccante potrebbe confermare le transazioni malevoli, riscrivere la storia della blockchain e prendere il controllo della rete. Per effettuare un attacco del 51%, l'attaccante deve possedere una quantità significativa di risorse, come potenza di calcolo, energia elettrica e denaro per sostenere l'attacco.

* + In questo caso, si parla di *hashrate* per definire la velocità con cui un dispositivo calcola e completa l’operazione. Essendo la rete bitcoin alla base decentralizzata ed essendo basato principalmente sulla potenza piuttosto che sulla parità, potrebbe ben accadere che un dispositivo generi blocchi più velocemente degli altri, risultando quindi un problema per gli utenti onesti.
  + L'attacco Finney (Finney Attack) può essere definito come un'estensione dell'attacco selfish mining. L'attaccante estrae un blocco furtivamente e invia la transazione non confermata all'altro nodo, eventualmente a un nodo commerciante. Se il nodo commerciante accetta la transazione, l'attaccante può aggiungere un nuovo blocco alla catena in un lasso di tempo ridotto, invertendo la transazione e inducendo un attacco di doppia spesa. La finestra di attacco nel caso di un attacco Finney è notevolmente ridotta, ma può causare molti danni se il valore della transazione è sufficientemente grande.

Altro tipo di attacco comune è l’attacco Sybil, un attaccante crea molteplici identità o nodi sulla rete per aumentare la propria potenza di calcolo. In questo modo, l'attaccante può aumentare le proprie possibilità di risolvere i problemi matematici e prendere il controllo della rete. Una debolezza in un nodo può essere un motivo per generare un attacco in un qualsiasi momento, così come punti in cui si ha avuto molto guadagno.

* Ne distinguiamo due tipi:
  + *Direct Sybil Attack*, che si verifica quando un nodo maligno interagisce direttamente con i nodi onesti del protocollo. Questo tipo di attacco è particolarmente efficace perché i nodi autentici non sono in grado di rilevare che i nodi falsi non sono legittimi. Di conseguenza, l'attaccante può manipolare i nodi autentici inducendoli a intraprendere azioni in linea con i propri interessi.
  + *Indirect Sybil Attack,* che si verifica quando i nodi falsi entrano in contatto con uno o più nodi collegati ai nodi autentici. A differenza dell'attacco sibillino diretto, gli hacker utilizzano nodi intermediari/proxy per lanciare un attacco indiretto. I nodi intermedi, che sono posizionati tra il nodo sibilo e quelli onesti, rappresentano uno o più punti di fallimento. Sfruttando questi nodi intermedi, gli hacker possono sferrare un attacco ai nodi onesti che non è facilmente individuabile come un attacco sibillino diretto.
  + Oltre ad essere un problema di privacy e che potenzialmente può portare al dominio della rete con un attacco simile a quello precedente. Similmente, alcuni nodi falsi possono rifiutarsi di aggiungere nuovi blocchi alla catena (“block withholding attack”); in questo modo, si manderà in bancarotta un pezzo della rete, dato che declina l’invio di nuovi profitti.
  + Un modo per contrastare questo tipo di attacco può essere l’autenticazione diretta fornendo dettagli reali (diretta) oppure validando le proprie informazioni personali a nodi considerati verificatori (indiretta). Un altro modo può essere lo stabilire un sistema gerarchico (dato che nuovi nodi o identità possono essere nodi Sybil) oppure creare dei grafi di fiducia sociale
* Un estensione del Sybil Attack è Timejacking Attack (Attacco a tempo), in cui ogni nodo mantiene un contatore di tempo che si basa sull'ora mediana dei suoi pari; se l'ora mediana differisce dall'ora del sistema di un certo valore, il nodo ritorna all'ora del sistema. Un aggressore può inondare la rete di nodi che riportano timestamp imprecisi, il che può causare un rallentamento o un'accelerazione della rete, portando a una desincronizzazione.

Un altro tipo di attacco comune è l’Eclipse attack (attacco Eclipse), che è un tipo di attacco che prende di mira una rete blockchain isolando un nodo specifico dal resto della rete. L'attacco prende il nome dall'evento astronomico che vede un corpo celeste bloccato o oscurato da un altro oggetto, come il sole oscurato durante un'eclissi solare.

* In un attacco Eclipse, un attaccante prende di mira un nodo specifico della rete blockchain e lo inonda di nodi falsi (*sybil nodes*, come visto sopra) controllati dall'attaccante. Questi nodi sibillini formano quindi una rete attorno al nodo preso di mira, isolandolo di fatto dal resto della rete. Una volta isolato il nodo preso di mira, l'aggressore può manipolare le informazioni che scorrono tra il nodo preso di mira e il resto della rete.
* Ad esempio, se una catena ha un nodo che ha solo otto connessioni in uscita e può supportare al massimo 128 thread in qualsiasi momento, ogni nodo ha accesso alla vista solo dei nodi ad esso collegati. La vista della catena per il nodo vittima può essere modificata se un attaccante attacca un nodo specifico e ottiene il controllo degli otto nodi ad esso collegati. Questo può portare a un'ampia varietà di danni, tra cui il doppio esborso di monete ingannando la vittima che una particolare transazione non si è verificata, e anche gli attacchi contro i protocolli di secondo livello.



Riferimento: <https://wesecureapp.com/blog/attacks-on-blockchain/>

* Per prevenire un attacco Eclipse, le reti blockchain possono implementare misure quali la limitazione del numero di connessioni che un nodo può avere, l'uso di reti peer-to-peer affidabili e l'utilizzo di più fonti per verificare l'autenticità delle informazioni. È inoltre importante che i nodi siano aggiornati con le ultime patch di sicurezza e che gli utenti evitino di utilizzare reti Wi-Fi pubbliche o connessioni non sicure per accedere alle reti blockchain.

## 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.

### Tipi di transazioni

Vi sono due tipi di transazioni: la transazioni P2PKH (Pay-to-PubKey-Hash) e le transazioni Coinbase.

* Le transazioni P2PKH (Pay-to-PubKey-Hash) sono il tipo più comune di transazioni utilizzate nella blockchain di Bitcoin e in molte altre criptovalute. In queste transazioni, il mittente invia una certa quantità di criptovaluta a un indirizzo Bitcoin. Questo indirizzo è una stringa alfanumerica che rappresenta la chiave pubblica del destinatario, che a sua volta è stata crittografata tramite la funzione hash SHA-256.
  + Per creare una transazione P2PKH, la persona che riceverà i fondi condivide il proprio portafoglio Bitcoin con il mittente. Si noti che un indirizzo è diverso da un hash a chiave pubblica. Un indirizzo codifica un hash a chiave pubblica in un formato facile da condividere e ha un rilevamento degli errori incorporato, oltre a un indicatore all'inizio che denota a quale rete appartiene. Il rilevamento degli errori avviene tramite una somma di controllo (talvolta chiamata somma di hash) che aiuta il software del portafoglio a rilevare un errore di battitura e ad evitare che i fondi vadano persi per sempre.
  + La conversione di una chiave pubblica in un indirizzo richiede che la chiave pubblica sia hashata due volte con due funzioni di hash diverse (SHA-256 per la prima e RIPEMD-160 per la seconda). Questo permette la creazione della transazione P2PKH
  + La conversione dell'hash della pubkey in un indirizzo richiede altri passaggi. Innanzitutto, i byte della versione (normalmente 0x00) vengono aggiunti all'inizio dell'hash della pubkey. Questa nuova stringa viene poi sottoposta a un nuovo hash con SHA-256. I primi quattro byte (32 bit) dell'hash risultante vengono aggiunti alla fine dell'hash RIPEMD-160 precedente. Questo funge da checksum. Quindi l'intera stringa viene convertita da una stringa di byte in una stringa con codifica base58. Il risultato è un indirizzo.
* Le transazioni Coinbase (dette anche transazioni di generazione) sono invece un tipo speciale di transazione che viene creata ogni volta che un nuovo blocco viene aggiunto alla blockchain. Questa transazione contiene una ricompensa in Bitcoin che viene assegnata al minatore che ha creato il blocco. In altre parole, è la transazione che crea nuovi Bitcoin e che permette di incentivare la partecipazione dei minatori alla rete. La transazione Coinbase non ha un mittente effettivo, in quanto viene creata direttamente dal protocollo della criptovaluta e non richiede una firma digitale.
  + Per evitare che la ricompensa resti sempre la stessa, il sistema è programmato per generare questo tipo di transazioni secondo una serie geometrica

## 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.
  + Ci sono alcuni tipi di valute diverse da Bitcoin:
    - Le altcoin, tutte le criptovalute che non sono Bitcoin. Di queste distinguiamo:
    - Le stablecoins, quindi criptovalute che seguono il prezzo del loro asset; non mantengono lo stesso valore e vengono usate per risparmi o per inviare denaro
    - Le mining-based, basandosi sul mining per verificare le transazioni
    - Le staking-based, per verificare transazioni ed aggiungere più monete a quelle disponibili
  + Alcune precisazioni per quanto riguarda le transazioni bitcoin:
    - Quando vengono spesi soldi da una delle parti, esiste uno script di firma contenente la chiave pubblica di Alice e la firma digitale delle transazioni ricevute generate dalla chiave privata, cioè *ScriptSig*.
      * Esso è uno script di input che viene incluso in una transazione Bitcoin per sbloccare i fondi precedentemente bloccati in un'uscita di transazione precedente (un input di transazione). Lo ScriptSig contiene i dati di input necessari per sbloccare l'output della transazione precedente, come ad esempio una firma digitale generata con la chiave privata del mittente.
    - *ScriptPubKey*, invece, è uno script di output che viene incluso nella transazione che crea un nuovo output bloccando dei fondi. Lo ScriptPubKey contiene le istruzioni per bloccare i fondi, specificando le condizioni che il destinatario deve soddisfare per sbloccare quei fondi in futuro. Ad esempio, lo script potrebbe richiedere che il destinatario fornisca una firma digitale valida generata con la sua chiave pubblica, che deve corrispondere alla chiave pubblica inclusa nello script.
    - Quando una transazione viene elaborata, il contenuto dello ScriptSig e dello ScriptPubKey viene combinato per formare uno script completo. Se lo script completo restituisce un valore booleano vero, la transazione viene considerata valida e i fondi vengono sbloccati e trasmessi al destinatario. Se il valore booleano è falso, la transazione viene considerata non valida e i fondi rimangono bloccati nella transazione precedente.
* 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.
* Litecoin
* Dogecoin
* Monero

## Wallet: tipi, chiavi, crittografia a chiave pubblica

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.

* L’indirizzo è la sola informazione per poter ricevere un pagamento e sarà composto da 27-34 caratteri alfanumerici. La chiave privata è invece composta da 51 caratteri.
* 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.
* Esistono anche dei wallet deterministici, che rappresentano una possibile soluzione ai rischi di furto dato che generano un numero infinito di chiavi da un unico codice seme (seed); da esso, quando salvato, saranno generati chiavi ed indirizzi.

### Crittografia nelle blockchain

Come sopra descritto, si tratta di avere una coppia chiavi pubblica e privata (quindi asimmetrica), fatta di una chiave distribuita ed una chiave personale/segreta, al fine di poter permette senza scambio di informazioni sul canale di comunicazione l’autenticità dell’informazione, rendendo valida l’informazione trasmessa (*integrità*), dando garanzie sull’identità delle parti in gioco (*autenticazione*) e proibendo di negare la transazione, anzi validandola subito (*non ripudiabilità*).

* Un algoritmo usato, ad esempio sulla rete Bitcoin, è l’algoritmo di firma digitale su Curve Ellittiche (ECDSA) è un meccanismo crittografico utilizzato per garantire l'autenticità e l'integrità delle transazioni nella blockchain. L'ECDSA utilizza una coppia di chiavi crittografiche, una pubblica e una privata, come nella firma asimmetrica tradizionale.
* L'ECDSA funziona utilizzando le proprietà matematiche delle curve ellittiche. In pratica, la chiave privata dell'utente viene utilizzata per generare una firma digitale univoca per la transazione. Questa firma viene quindi verificata utilizzando la chiave pubblica dell'utente.
* L'ECDSA viene utilizzato in diverse blockchain, tra cui Bitcoin, per garantire la sicurezza e l'integrità delle transazioni. In particolare, l'ECDSA viene utilizzato nella verifica delle firme digitali delle transazioni nella blockchain Bitcoin.
* Quando un utente invia una transazione Bitcoin, questa viene firmata digitalmente utilizzando la chiave privata dell'utente e l'algoritmo ECDSA. La firma digitale viene quindi trasmessa alla rete Bitcoin insieme alla transazione. Quando la transazione viene ricevuta dalla rete, la firma viene verificata utilizzando la chiave pubblica dell'utente. Se la verifica è positiva, la transazione viene considerata valida e aggiunta alla catena di blocchi.

Ricapitoliamo quanto detto sopra con un esempio pratico di utilizzo di crittografia asimmetrica nelle transazioni blockchain è quello che avviene quando un utente A invia una transazione a un utente B sulla blockchain.

* Innanzitutto, l'utente A utilizza la sua chiave privata per firmare digitalmente la transazione. La firma digitale viene poi trasmessa insieme alla transazione alla rete blockchain.
* Quando la transazione viene ricevuta dalla rete, la chiave pubblica dell'utente A viene utilizzata per verificare la firma digitale. Se la firma è valida, la transazione viene aggiunta alla catena di blocchi e viene trasmessa all'utente B.
* L'utente B può quindi utilizzare la chiave pubblica dell'utente A per verificare l'autenticità della transazione e la validità della firma digitale. In questo modo, l'utente B può essere certo che la transazione è stata effettivamente inviata dall'utente A e che non è stata alterata durante il processo di trasmissione.

Un esempio di curva che usa ECDSA è *Secp256k1* è il nome della curva ellittica utilizzata da Bitcoin per implementare la sua crittografia a chiave pubblica. Tutti i punti di 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 elevato, per il Punto Generatore, un punto definito sulla curva secp256k1.

La curva Secp256k1 è definita su un campo finito di 256 bit ed è rappresentata dall'equazione:

dove p è un numero primo molto grande e le coordinate x e y sono interi nel campo finito definito da p.

Questa curva ellittica viene usata dato che non ha una struttura “del tutto” casuale, ma grazie alle costanti e , il modulo del campo, punto base della curva e ordine del punto base, è possibile accelerare i calcoli essendo la funzione dipendente da questa serie di parametri. Grazie alla scelta di numeri grandi, si garantisce sicurezza e un calcolo più veloce nelle sue parti.

* Molto usate anche le funzioni di hash, che non sono iniettive e hanno la proprietà di non permettere di trovare due controimmagini diverse per una stessa immagine (preimage resistant). Il loro principale vantaggio è essere calcolate in modo efficiente; data infatti una stringa di qualsiasi lunghezza, si vuole generare un *digest* di messaggio a lunghezza fissata, definito come . Come detto sopra, sono facilmente rimodificabili; ciò rende difficile la collisione, cioè avere due stringhe di hash uguali generate da due stringhe diverse in partenza (quindi, due stringhe

In particolare hanno i seguenti effetti:

* + Effetto valanga (avalanche effect)- Una piccola modifica dei dati può produrre un risultato significativamente diverso.
  + Unicità - Ogni input ha un output unico.
  + Determinismo - Qualsiasi input avrà sempre lo stesso output se passato attraverso la funzione hash.
  + Rapidità - L'output può essere generato in un tempo molto ridotto.
  + Non è possibile il reverse engineering, cioè non si può generare l'input avendo a disposizione l'output e la funzione hash.
  + Gli algoritmi più usati a livello hash nelle blockchain sono:
    - *SHA-256* (Secure Hash Algorithm 256), che utilizza una rete di funzioni di compressione, chiamate "funzioni di compressione di blocco", per elaborare i dati di input e produrre un hash di 256 bit come output. La funzione di compressione prende in input un blocco di dati di 512 bit e produce un hash di 256 bit. La funzione di compressione utilizza una combinazione di operazioni logiche, tra cui l'operazione XOR (or esclusivo), l'operazione AND (and logico), l'operazione NOT (not logico) e l'operazione ADD (somma) per produrre l'hash finale.
    - *SHA-3* (Secure Hash Algorithm 3), funzione di hashing crittografica alternativa a SHA-256, sviluppata dal National Institute of Standards and Technology (NIST). SHA-3 è basato su un algoritmo chiamato Keccak, che utilizza una struttura a "sponge function" per produrre l'hash.
      * La funzione di hash SHA-3 utilizza un'operazione di permutazione non lineare per manipolare i dati di input. Durante l'elaborazione, i dati vengono assorbiti in un "sponge", ovvero una struttura di dati che viene manipolata tramite l'operazione di permutazione. Una volta che i dati sono stati completamente assorbiti, l'output viene estratto dallo sponge.
    - L'algoritmo di hash RIPEMD-160 è una funzione di hashing crittografica che viene utilizzata in diverse criptovalute, tra cui Bitcoin. Il suo nome deriva dalla sua struttura "RACE Integrity Primitives Evaluation Message Digest" e dalla sua lunghezza di output di 160 bit.
      * L'algoritmo di hash RIPEMD-160 è basato su una rete di funzioni di compressione, che utilizza una combinazione di operazioni di permutazione, rotazione e operazioni logiche per produrre l'output finale. La funzione di compressione prende in input un blocco di dati di 512 bit e produce un hash di 160 bit.
      * La funzione di compressione consiste di due fasi principali: una fase di pre-processing e una fase di elaborazione. Durante la fase di pre-processing, il blocco di dati viene diviso in 16 parole da 32 bit ciascuna e queste parole vengono mescolate e manipolate tramite operazioni di permutazione e rotazione. Durante la fase di elaborazione, le parole vengono sottoposte a diverse operazioni logiche, tra cui l'operazione XOR (or esclusivo), l'operazione AND (and logico), l'operazione NOT (not logico) e l'operazione ADD (somma).
      * L'output dell'algoritmo di hash RIPEMD-160 è una stringa di 160 bit che rappresenta l'hash del messaggio originale. L'hash viene utilizzato per garantire l'integrità e la sicurezza dei dati nella blockchain, poiché qualsiasi modifica ai dati originali comporterebbe una modifica all'hash corrispondente.
  + Sono usate alcune strutture per verificare l’integrità dei dati; un esempio sono gli *alberi di Merkle*, la cui idea è di suddividere i dati in blocchi più piccoli e di calcolare l'hash di ciascun blocco. Gli hash dei blocchi vengono poi combinati a coppie e nuovamente "hashati" fino a quando non rimane un solo hash, noto come root hash o Merkle root. L'albero di Merkle può essere rappresentato come un albero binario in cui le foglie rappresentano gli hash dei blocchi e i nodi intermedi rappresentano gli hash delle coppie di blocchi.
  + L'utilizzo dell'albero di Merkle consente di verificare l'integrità di una grande quantità di dati in modo efficiente. Infatti, invece di dover verificare l'integrità di tutti i dati, è sufficiente verificare l'integrità del Merkle root. Se il Merkle root viene alterato, anche gli hash dei blocchi vengono alterati e di conseguenza viene rilevata una violazione dell'integrità.
  + Gli alberi di Merkle sono ampiamente utilizzati nella blockchain, in cui i blocchi sono composti da un gran numero di transazioni. In particolare, il Merkle root viene incluso nell'header di ogni blocco e consente di verificare l'integrità di tutte le transazioni contenute nel blocco. In questo modo, gli utenti della blockchain possono essere certi che le transazioni sono state eseguite correttamente e che non sono state alterate.

## Mining dei blocchi

* Ci sono vari modi di guadagnare criptovalute:
  + Vendere beni o servizi ed essere ricompensati con la valuta di interesse
  + Accedere a servizi di cambi valute reali-cripto
  + Partecipare al protocollo di validazione/inserimento transazioni sulla rete, ottenendo una commissione per ogni transazione trattata; ogni 10 minuti vengono generate e generate nuove cripto (caso Bitcoin) e chi risolve per primo il processo di creazione di nuovi blocchi risolvendo un problema crittografico ne viene ricompensato; è quello che approfondiremo in questa sezione
* 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. Un computer normale potrebbe non esserne pienamente in grado; per esempio, si tratterebbe di individuare il numero corretto tra 4 miliardi di possibilità. Il fatto di avere correttamente individuato il blocco dona criptovalute o ricompense similari.
* 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/>

### Considerazioni sul mining

Il mining nel contesto della blockchain e delle criptovalute si riferisce al processo di aggiunta di nuove transazioni alla blockchain attraverso l'uso della potenza di calcolo per risolvere complessi problemi matematici. Questo processo richiede una quantità significativa di energia, che può portare a preoccupazioni circa il suo impatto ambientale.

Alcuni sostengono che il mining è volutamente dispendioso perché la difficoltà dei problemi matematici da risolvere è intenzionalmente elevata per limitare la velocità di aggiunta di nuovi blocchi alla blockchain. Questo crea una competizione tra i minatori per risolvere questi problemi il più velocemente possibile, il che fa aumentare il consumo di energia in quanto i minatori utilizzano sempre più potenza di calcolo per cercare di superarsi a vicenda.

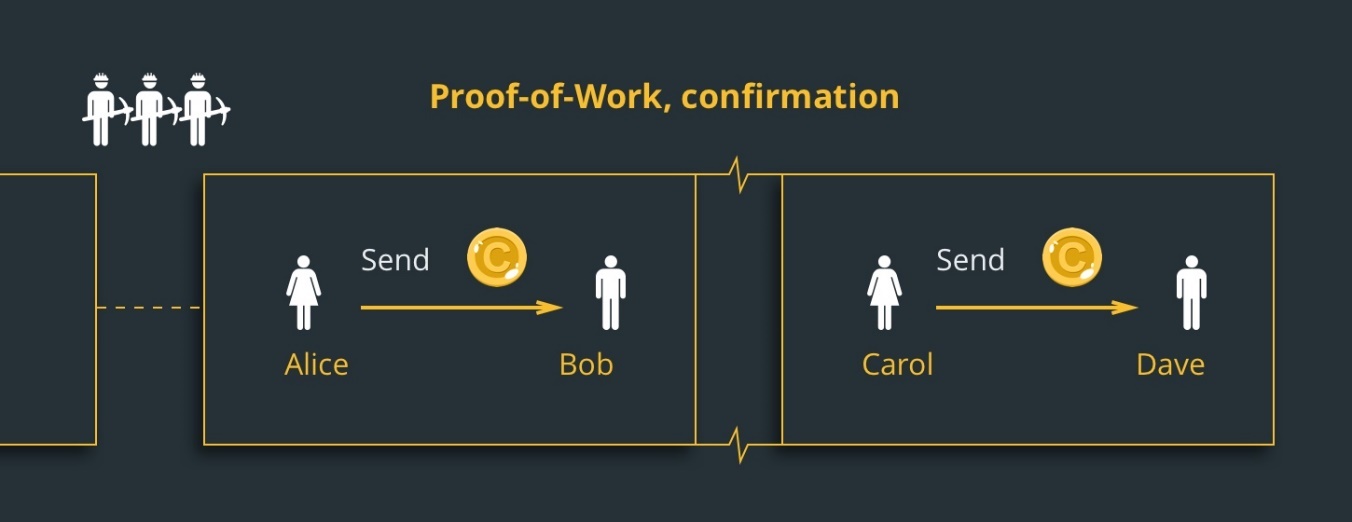
Tuttavia, è importante notare che il consumo di energia associato all'attività di mining non è del tutto dispendioso, in quanto ha un'importante funzione di protezione della rete blockchain e di prevenzione delle frodi. Inoltre, alcuni sostengono che, man mano che le fonti di energia rinnovabile diventano più diffuse e convenienti, l'impatto ambientale del mining diminuirà. Inoltre, è certamente più economico dell’impiego di personale umano e previene i malintenzionati.

Nel complesso, sebbene vi siano valide preoccupazioni sull'impatto ambientale dell'attività di mining nel contesto della blockchain e delle criptovalute, non è esatto affermare che si tratti di uno spreco intenzionale. La complessità dei problemi matematici da risolvere è una componente necessaria della sicurezza della blockchain e si stanno compiendo sforzi per rendere il mining più efficiente dal punto di vista energetico e sostenibile per l'ambiente.

## Algoritmi di consenso

### Proof of Work

Il Proof of Work (PoW) (noto anche come mining in effetti, ma ha un suo significato separato e preciso) è un algoritmo di consenso utilizzato dalle blockchain per confermare la validità delle transazioni e creare nuovi blocchi. Il PoW è stato introdotto per la prima volta con la creazione di Bitcoin, ma è stato successivamente adottato da numerose altre criptovalute e blockchain.



Riferimento: <https://cointelegraph.com/explained/proof-of-work-explained>

* In poche parole, il Proof of Work funziona in questo modo: i partecipanti alla rete, detti miner, risolvono un complesso problema matematico per creare un nuovo blocco di transazioni sulla blockchain. Il problema matematico consiste nella ricerca di un hash (una stringa di numeri e lettere) che soddisfa una determinata condizione, detta target. La condizione target richiede che l'hash del nuovo blocco sia inferiore a un determinato valore. Questo valore viene stabilito in base alla difficoltà della blockchain, che viene regolata automaticamente per mantenere il tempo medio di creazione di un nuovo blocco costante. Di fatto:
  + Ogni qual volta si invii una transazione, la rete richiede 10 minuti circa per confermarla e può gestire circa sette transazioni al secondo. Entro questi dieci minuti si forma un nuovo blocco
  + Ogni blocco detiene diverse transazioni, che devono essere validate in modo indipendente
  + I miners, con più alto rendimento computazionale, prendono una transazione alla volta e risolvono un algoritmo crittografico, altrimenti noto come proof of work
  + La transazione, a questo punto viene validata e pubblicata sulla blockchain pubblica affinché tutti possano vederla. I miners più veloci, i primi che risolvono l’algoritmo, vengono ricompensati in criptovalute, quella di utilizzo della blockchain su cui operano. Di fatto, quindi, non è una cosa equa, in quanto si consuma molta energia ed è pesantemente sbilanciata a favore di chi abbia le attrezzature migliori
  + Di fatto, il meccanismo di validazione è molto lento. Le transazioni sono memorizzate in una mempool in attesa di convalida, con tempi medi di conferma tra il 1° gennaio e il 9 febbraio 2023 che vanno da sette a 91 minuti (la conferma è quando la transazione viene confermata).
    - Una *mempool* (o txpool) è l’area in cui si trovano le transazioni che non sono state aggiunte ad un blocco e sono tuttora non state confermate. Questa area di attesa o zona cuscinetto è necessaria perché le transazioni non vengono aggiunte immediatamente alla Blockchain.
    - I nodi eseguono anche una serie di controlli di validità su queste transazioni. Questi controlli includono la verifica che i fondi siano ancora disponibili, che l'output non superi l'input, che la firma sia valida, ecc. La transazione viene rifiutata se non supera uno di questi test.
    - Si noti che il Mempool non può essere considerato come un riferimento principale condiviso universalmente da tutti i nodi. Ogni nodo configura le proprie regole per il suo mempool. Inoltre, un nodo può essere il primo a ricevere una transazione, ma potrebbe non averla propagata al resto della rete.
  + Tuttavia, l’algoritmo di consenso PoW Proof of Work consente ai miners di convalidare un nuovo blocco e aggiungerlo alla blockchain solo se gli altri nodi del network concordano con la soluzione fornita dal miner, ripetendo l’operazione risolta.

La Proof-of-Work è utilizzata in molte criptovalute.

* L'applicazione più famosa di PoW è Bitcoin. È stato Bitcoin a gettare le basi per questo tipo di consenso. Il puzzle è Hashcash. Questo algoritmo consente di modificare la complessità di un puzzle in base alla potenza totale della rete. Il tempo medio di formazione dei blocchi è di 10 minuti. Le criptovalute basate su Bitcoin, come Litecoin, hanno un sistema simile.
* Un altro grande progetto con PoW è Ethereum. Dato che quasi tre progetti su quattro sono implementati sulla piattaforma Ethereum, si può affermare che la maggior parte delle applicazioni Blockchain utilizza il modello di consenso PoW.

I vantaggi principali sono la difesa dagli attacchi DoS e il basso impatto della posta in gioco sulle possibilità di estrazione.

* Difesa dagli attacchi DoS. Il PoW impone alcuni limiti alle azioni nella rete. Per essere eseguite necessitano di un grande impegno. Un attacco efficiente richiede molta potenza di calcolo e molto tempo per eseguire i calcoli. Pertanto, l'attacco è possibile ma piuttosto inutile, poiché i costi sono troppo elevati.
* Possibilità di estrazione. Non importa quanto denaro avete nel vostro portafoglio. Ciò che conta è avere una grande potenza di calcolo per risolvere i puzzle e formare nuovi blocchi. In questo modo, i detentori di ingenti somme di denaro non sono incaricati di prendere decisioni per l'intera rete.

#### Puzzle matematici della PoW

Ce ne sono molti, ad esempio:

* *funzione hash*, ovvero come trovare l'input conoscendo l'output.
  + Queste funzioni non sono reversibili, dato che sarebbe impossibile ottenere il dato originale di input dall’output della funzione di hash. Le funzioni sono infatti designate per essere a via unica. La computazione è molto più semplice in avanti che all’indietro.
* *fattorizzazione di interi* (prime/integer factorization), in altre parole, come presentare un numero come moltiplicazione di altri due numeri.
  + I numeri primi sono tutti i numeri divisibili solo per sé stessi e per 1

Una pratica comune è quella di utilizzare semi-primi molto grandi (cioè il risultato della moltiplicazione di due numeri primi) come numero di sicurezza della crittografia. Per decifrarlo, si dovrebbe trovare la fattorizzazione prima del numero semiprimo grande, cioè due o più \*\*numeri primi\*\* che moltiplicati insieme danno come risultato il numero originale.

Normalmente è facile generare un numero primo grande, ma fattorizzarlo richiede un processo di trial-and-error non indifferente

* + Algoritmi crittografici come RSA, che si basa sulla moltiplicazione di due numeri primi (P e Q) per ottenere il valore del modulo (N). Ci possono essere attacchi al valore del modulo; normalmente, si cercano una serie di numeri primi che permettano di ottenere , ottenuta come . Ci sono vari modi per realizzare questo attacco, ad esempio tramite:
    - La differenza di quadrati
    - Residui quadratici mod n
    - Fattorizzazione di curve ellittiche
    - Il metodo di Pollard
* protocollo puzzle di visita guidata (guided tour puzzle protocol). Se il server sospetta un attacco DoS, richiede il calcolo delle funzioni hash per alcuni nodi in un ordine definito. In questo caso, si tratta di un problema di "come trovare una catena di valori di funzioni hash".
  + Ecco come funziona il protocollo dei puzzle delle visite guidate:
    - Il mittente genera una serie di enigmi, ciascuno con una soluzione unica. I puzzle sono progettati in modo da essere computazionalmente difficili da risolvere, ma facili da verificare.
    - Il mittente invia l'insieme dei puzzle al destinatario.
    - Il destinatario seleziona uno dei puzzle e lo risolve. La soluzione del rompicapo serve come biglietto o chiave per accedere al canale di comunicazione.
    - Il ricevitore invia la soluzione al mittente.
    - Il mittente verifica la soluzione e concede l'accesso al canale di comunicazione.
    - Il mittente e il destinatario possono ora comunicare in modo sicuro utilizzando tecniche di crittografia e decrittografia.
    - Il protocollo del puzzle di visita guidata è progettato per impedire agli aggressori di intercettare e leggere la comunicazione tra il mittente e il destinatario. Anche se un aggressore intercettasse l'insieme dei puzzle, sarebbe computazionalmente impossibile risolvere tutti i puzzle per trovare la soluzione corretta. Pertanto, il protocollo garantisce che solo il destinatario previsto possa accedere al canale di comunicazione.

#### Tipi di PoW

##### Proof of Meaningful Work (PoMW)

Il Proof of Meaningful Work (PoMW) è un algoritmo di consenso che cerca di combinare i vantaggi di Proof of Work (PoW) e Proof of Stake (PoS), cercando di mitigare i loro svantaggi. In PoMW, i partecipanti alla rete devono svolgere un lavoro utile per risolvere un problema specifico (progetti scientifici, es. ricerca medica per cure, ricerca chimica, ricerca astrofisica, etc.) in modo da dimostrare di aver svolto "un lavoro significativo" che richiede una quantità significativa di potenza di elaborazione.

* Ciò significa che i partecipanti alla rete che svolgono il lavoro ricevono una ricompensa per la loro fatica, in modo simile a PoW, ma evitando di utilizzare una quantità enorme di energia come avviene in PoW.
* Consuma meno rispetto a PoW ed è più equo rispetto a PoS e si ha un riconoscimento del lavoro svolto dai partecipanti
* Tuttavia, vi è la possibilità che partecipanti alla rete possano cercare di "imbrogliare" il sistema svolgendo il lavoro in modo inefficiente o in modo tale da ottenere il maggior numero possibile di ricompense.

##### Hybrid Proof of Work (HPoW)

L’Hybrid Proof of Work (HPoW) è un'altra variante dell'algoritmo PoW che cerca di ridurre i suoi svantaggi. In HPoW, gli utenti partecipano alla creazione di nuovi blocchi condividendo potenza di elaborazione, come avviene in PoW. Tuttavia, a differenza di PoW tradizionale, HPoW richiede anche la partecipazione dei possessori di token, come avviene in PoS, per validare i blocchi. Questo significa che l'algoritmo è meno suscettibile alle attività di mining centralizzate che possono verificarsi in PoW tradizionale, senza sacrificare la sicurezza del network come avviene in PoS.

* HPoW elimina l'incentivo al profitto per i minatori perché la ricompensa per l'estrazione è così bassa.
* Un singolo minatore non può vincere più di una volta ogni 30 minuti.
* Il saldo dell'indirizzo di ricompensa del minatore deve essere maggiore o uguale a una quantità minima di Lynx richiesta e fluttuante per vincere un blocco.
* Utilizzando una selezione casuale, i minatori più veloci non hanno sempre la garanzia di vincere la ricompensa del blocco.
* Risulta più sicuro rispetto a PoS e consuma meno rispetto a PoW, ma può essere vulnerabile alla concentrazione di potere da parte dei possessori di token.
* Di fatto, viene usato dalla criptovaluta Lynx

##### Delayed Proof of Work (dPoW)

La Delayed Proof of Work (dPoW) è un metodo di consenso ibrido che consente a una blockchain di sfruttare la sicurezza fornita dalla potenza di hashing di una blockchain secondaria. Ciò avviene attraverso un gruppo di nodi notarili (notary nodes) che aggiungono dati dalla prima blockchain alla seconda, il che richiederebbe la compromissione di entrambe le blockchain per minare la sicurezza della prima.

* Viene usato nelle blockchain Komodo. Il processo di inserimento dei backup delle transazioni di Komodo in un PoW sicuro è la "notarizzazione". La notarizzazione viene eseguita dai nodi notarili eletti. All'incirca ogni dieci minuti, i nodi notarili eseguono uno speciale hash dei blocchi estratto sulla blockchain di Komodo e prendono nota dell'"altezza" complessiva della blockchain di Komodo.
* I nodi notarili elaborano questo blocco specifico in modo che le loro firme siano incluse crittograficamente nel contenuto dei dati autenticati. In questo modo, a basso costo è possibile minare e ritrovare le giuste informazioni di riferimento.

### Proof of Stake

La Proof of Stake (PoS) è un algoritmo di consenso utilizzato in alcune criptovalute per raggiungere un accordo sulla validità delle transazioni e delle operazioni nella blockchain. La PoS funziona in modo diverso dalla Proof of Work (PoW) utilizzata in criptovalute come Bitcoin.

* Invece di affidarsi alla potenza di calcolo per risolvere complessi problemi matematici, come avviene nella PoW, la PoS si basa sulla detenzione di una certa quantità di criptovaluta come garanzia per la validazione delle transazioni. In pratica, i nodi della rete bloccano una certa quantità di criptovaluta come "punteggio" per dimostrare che hanno un interesse nella corretta validazione delle transazioni. Questo punteggio viene utilizzato come base per la selezione del nodo che convalida la transazione successiva.
* A differenza del PoW, non ci sono miner coinvolti nel processo. Al loro posto, i partecipanti alla rete che vogliono essere coinvolti nella verifica della validità delle transazioni e nella creazione di blocchi nella rete devono detenere una certa quota nella rete, per esempio mettendo una certa quantità di moneta della rete in un portafoglio collegato alla sua blockchain. Questo processo è noto come "placing a stake" o "staking”, che può essere tradotto come il fatto di mettere i propri interessi in gioco. Un creatore di blocchi in un sistema PoS può solo creare blocchi proporzionati alla propria partecipazione alla rete.
* Pertanto, le reti PoS sono basate su algoritmi deterministici, il che significa che i validatori dei blocchi sono eletti a seconda della natura della posta in gioco. Per esempio, selezionare il saldo del conto come unico criterio su cui viene definito il prossimo blocco valido in una blockchain potrebbe potenzialmente portare a una centralizzazione indesiderata. Ciò vorrebbe dire che i membri ricchi di una rete godrebbero di grandi vantaggi.

A livello di vantaggi:

* La PoS ha il vantaggio di essere meno intensiva in termini di energia rispetto alla PoW e richiede meno potenza di calcolo per mantenere la sicurezza della rete. Inoltre, la PoS è meno vulnerabile ad attacchi del 51 percento rispetto alla PoW, poiché gli attaccanti dovrebbero possedere la maggioranza delle criptovalute della rete, e non la maggioranza della potenza di calcolo.
* Migliora il decentramento e democratizza l’accesso alla rete (permettendo a tutti di accedere), è più scalabile e anche sicura, dato che la quantità di criptovaluta viene usata come garanzia per partecipare al processo di consenso e riducendo il rischio di comportamenti fraudolenti.

A livello di svantaggi:

* I produttori di blocchi di alcune monete possono esercitare una quantità incredibile di potere se il numero di produttori di blocchi in una rete è basso, e se quindi sono loro a poter convalidare tutte le transazioni. Tuttavia, il potere di un produttore può essere automaticamente revocato ogni volta che fa qualcosa contro gli interessi della rete. Se, per esempio, un produttore della moneta EOS non riesce a lavorare su nessun blocco per 24 ore, un produttore di riserva prende rapidamente il suo posto.
* La seconda grande debolezza è che un certo numero di sistemi PoS favorisce gli utenti ricchi: quante più monete si hanno in gioco nella rete, tanto più si estende il proprio diritto di voto. Reti come Cardano hanno già affrontato questo problema implementando la selezione randomizzata dei produttori di blocchi. In questo caso, gli utenti più ricchi hanno ancora una migliore possibilità di essere produttori di blocchi, ma è invece diminuita l'influenza esterna delle "cripto balene", ovvero dei partecipanti che detengono molte più monete di una particolare rete rispetto all'utente medio.
* Infine, una rete Proof of Stake ha un problema noto come "nessuna posta in gioco". In una rete PoW c’è l'eventualità che due miner producano un blocco quasi simultaneamente a causa di un ritardo temporale. Questo si traduce in una confusione temporanea nella rete e i nodi devono raggiungere il consenso su quale blocco sia valido. Di conseguenza, i miner devono scegliere su quale versione della blockchain spendere le loro risorse, bypassando le altre opportunità.

Molti hanno provato a risolvere questi problemi (di seguito alcune criptovalute)

* Peercoin ha messo in atto dei checkpoint firmati dalla chiave privata del programmatore e poi veicolati centralmente dal sistema. Ciascun checkpoint è un punto fermo e non può essere riorganizzato né esso stesso né tantomeno la parte “approvata” da esso. Lo sviluppatore, quindi, è l’autorità centrale che pesa estremamente sulla blockchain.
* Nxt consente di rilavorare un numero definito di blocchi: 720. Possibile conseguenza: il client potrebbe quindi “seguire” una ramificazione di 721 blocchi non accertandosi che sia la blockchain più lunga, prevenendo il consenso.
* Ethereum – Slasher: gli utenti possono “punire” un “imbroglione” che forgia sui forks (cambiamenti al protocollo non retrocompatibili) della blockchain. L’utente avrà dovuto firmare due volte per creare una biforcazione e sarà punito se avrà creato una biforcazione senza avere nessuna posta in gioco.

#### Delegated Proof of Stake

La Delegated Proof of Stake (DPoS) è una variante dell'algoritmo di consenso Proof of Stake (PoS) utilizzato in alcune criptovalute, come ad esempio EOS.

* A differenza della PoS tradizionale, dove tutti i nodi della rete possono partecipare al processo di validazione delle transazioni, nella DPoS vengono scelti un numero limitato di nodi (solitamente tra 20 e 100) come "delegati" che hanno il compito di convalidare le transazioni e aggiornare la blockchain. Questi delegati sono selezionati in base al numero di voti che ricevono dai detentori di criptovalute della rete.
* I voti sono proporzionali alla quantità di criptovaluta detenuta dai votanti e i delegati vengono scelti in ordine decrescente di voti ricevuti. I delegati eletti sono quindi responsabili della validazione delle transazioni e vengono ricompensati con le commissioni di transazione per il lavoro svolto.
* La DPoS ha alcuni vantaggi rispetto alla PoS tradizionale e alla Proof of Work (PoW). In primo luogo, la DPoS è più veloce e scalabile rispetto alla PoW, in quanto la selezione dei delegati è più efficiente rispetto al processo di mining. Inoltre, la DPoS riduce la centralizzazione, poiché solo un piccolo numero di nodi è coinvolto nel processo di convalida delle transazioni.
* Tuttavia, la DPoS ha anche alcune criticità. Innanzitutto, la selezione dei delegati è basata sulla quantità di criptovaluta detenuta, il che potrebbe creare disuguaglianze tra i detentori di criptovalute e potenzialmente portare alla creazione di oligarchie. Inoltre, i delegati potrebbero subire pressioni esterne per convalidare transazioni non valide o dannose.

#### Leased Proof of Stake (LPoS)

La Leased Proof of Stake (LPoS) è un meccanismo di consenso utilizzato in particolare dalla blockchain Waves, in base al quale gli utenti affittano token crittografici a un nodo che intende agire come produttore di blocchi della rete. Più token un nodo ha in palio, più è probabile che venga scelto per generare il blocco successivo e ricevere la ricompensa corrispondente, e i proprietari dei token hanno il diritto di cancellare il loro contratto di locazione in qualsiasi momento.

* Di conseguenza, i piccoli detentori di token che altrimenti non avrebbero diritto a partecipare al processo di creazione dei blocchi in un sistema PoS tradizionale possono unire le loro risorse e aumentare le possibilità di ricevere una quota delle commissioni di transazione della rete. Gli utenti possono fare acquisti per trovare il nodo che meglio si adatta alla loro strategia di investimento, poiché alcuni nodi possono distribuire ricompense maggiori.
* I protocolli LPoS si applicano meglio alle reti che hanno requisiti tecnici elevati per gestire un nodo completo in grado di convalidare le transazioni sulla catena. Questo meccanismo di consenso premia i nodi più performanti, incentivando gli utenti più piccoli a sostenere i validatori più efficienti in modo trasparente e sostenibile. In termini di effetto netto, questo meccanismo di consenso è abbastanza simile a DPoS. Tuttavia, mentre i validatori di DPoS sono selezionati dai voti ponderati degli altri partecipanti alla rete, i possessori di token all'interno di una rete LPoS possono prendere in prestito e prestare token direttamente per partecipare al processo di produzione dei blocchi.

#### Pure Proof of Stake (PPoS)

La Pure Proof of Stake (PPoS) è una forma altamente democratizzata di PoS utilizzata da Algorand, un progetto di blockchain pubblica incentrato sullo sviluppo di applicazioni decentralizzate (dApp) di facile utilizzo. A differenza di molte altre forme di PoS, i meccanismi di consenso PPoS non dispongono di un meccanismo di sanzione incorporato per prevenire l'attività di nodi maligni o potenziali difetti di sicurezza come la duplicazione delle convalide dei blocchi. Al contrario, PPoS offre requisiti minimi di puntata per la partecipazione e la sicurezza della rete, aprendo le porte a tutti gli utenti interessati. Questo crea un sistema in cui sarebbe finanziariamente autodistruttivo per gli attori disonesti interrompere o dirottare la rete.

* Sulla rete Algorand è necessaria una sola moneta ALGO per partecipare al processo di staking della rete. Ogni utente della rete Algorand può essere selezionato in modo casuale e segreto per proporre nuovi blocchi e votare le proposte, e la probabilità che un determinato utente venga scelto - insieme al peso delle sue proposte e dei suoi voti - è proporzionale alla sua partecipazione. Un sistema PPoS funzionerà normalmente finché due terzi dei nodi della rete agiranno onestamente.

### Alcune tipologie di consenso

#### Proof of Importance (PoI)

Nella Proof of Importance la partecipazione alla convalida della rete è basata sulla quantità di criptovaluta detenuta e sulla sua attività sulla rete. In pratica, i nodi con un saldo maggiore e un'attività più attiva sulla rete hanno maggiori probabilità di essere selezionati per la convalida delle transazioni.

* In altre parole, PoI valuta la "importanza" di un nodo sulla base del suo coinvolgimento nella rete, incentivando la partecipazione attiva degli utenti. PoI ha il vantaggio di essere meno vulnerabile agli attacchi del 51 percento rispetto alla PoW e alla PoS, poiché gli attaccanti dovrebbero possedere la maggioranza delle criptovalute della rete e un'attività molto elevata sulla rete per poter manipolare il processo di convalida.
* I criteri esatti di attribuzione dei punteggi utilizzati nei PoI variano, anche se molti di questi meccanismi di consenso prendono in prestito caratteristiche dagli algoritmi utilizzati nel clustering della rete e nel ranking delle pagine. Tra i fattori comuni vi sono il numero di trasferimenti a cui un nodo ha partecipato in un determinato periodo di tempo e il grado di interconnessione tra i diversi nodi attraverso i cluster di attività.
* Il PoI aiuta a mitigare il rischio di un eccesso di ricchezza concentrata, in quanto i maggiori detentori di token non esercitano un potere assoluto sulla rete. Poiché il punteggio di importanza di ciascun nodo è dinamico e basato sull'attività della rete, questo meccanismo di consenso scoraggia le biforcazioni della blockchain: Gli utenti dovrebbero spendere risorse per rimanere attivi su entrambe le reti biforcate al fine di mantenere il proprio punteggio.

#### Proof of Burn (PoB)

Il proof-of-burn (PoB) è un meccanismo di consenso della blockchain con un consumo energetico minimo, rispetto al proof-of-work (PoW). Le piattaforme decentralizzate che utilizzano il metodo PoB assicurano che i minatori raggiungano il consenso bruciando le monete. La masterizzazione è il processo di eliminazione permanente delle criptovalute dalla circolazione. Sebbene questa pratica riduca l'inflazione, le blockchain basate su PoB la utilizzano per convalidare le transazioni.

* In parole povere, i minatori PoB iniziano a bruciare monete virtuali come modo per dimostrare il loro coinvolgimento nella rete ed essere autorizzati a minare. Il numero di monete bruciate da un minatore dimostra la sua potenza mineraria virtuale. Pertanto, maggiore è il numero di monete, maggiore è la potenza e viceversa. Si noti che, proprio come nei sistemi PoW, una maggiore potenza di mining migliora la velocità di trovare nuovi blocchi. Di conseguenza, il minatore ottiene maggiori ricompense.
* Per bruciare le monete, i minatori le inviano a un indirizzo non spendibile e verificabile. Questo processo non consuma molte risorse (a parte le monete bruciate) e garantisce che la rete rimanga attiva e agile. A seconda dell'implementazione, i minatori possono bruciare la valuta nativa o la valuta di una catena alternativa, come Bitcoin. In cambio, ricevono una ricompensa in token della valuta nativa della blockchain. Nelle reti proof-of-burn (PoB), il processo di masterizzazione delle monete prevede l'invio delle stesse a un "indirizzo di eater". Questo indirizzo è pubblicamente verificabile ma inaccessibile. Si noti che gli indirizzi degli eater sono randomizzati e non hanno chiavi private.

#### Proof of Authority (PoA)

La Proof-Of-Authority (PoA) è un metodo di consenso che conferisce a un numero ristretto e designato di attori della blockchain il potere di convalidare le transazioni o le interazioni con la rete e di aggiornare il suo registro più o meno distribuito.

* Funziona come segue: in base allo schema scelto, una o più macchine validatrici sono responsabili della generazione di ogni nuovo blocco di transazioni che verrà inserito nella Blockchain. Il nuovo blocco può essere accettato direttamente senza verifica, o con voto unanime dei generatori di blocchi, o semplicemente a maggioranza, a seconda della configurazione scelta per la Blockchain. Questi nodi hanno il compito di validare le transazioni, creare nuovi blocchi e aggiornare il registro. Nel PoA, i nodi autorizzati sono motivati a fornire un servizio affidabile e sicuro, poiché il loro status di autorità dipende dalle loro prestazioni.
* Di fatto, mentre risulta molto veloce e scalabile dato che non richiede risoluzione di problemi complessi o sacrificio di cripto, risulta un sistema di consenso centralizzati, in quanto i nodi autorizzati sono selezionati e designati da un’autorità centrale, limitando la decentralizzazione. Inoltre, anche la sicurezza può essere ridotta, in quanto vulnerabile agli attacchi di coordinamento, dato che un attaccante potrebbe cercare di infiltrarsi nella rete diventando uno dei nodi autorizzati.

#### Tolleranza ai guasti bizantina (BFT)

Il problema che risolve è il Byzantine Generals Problem, 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.

La fault tolerance, per garantire il successo della squadra dei generali, richiede un algoritmo che rispetti le seguenti condizioni:

* Tutti i generali delle truppe devono essere d'accordo sulla prossima azione del piano.
* I generali devono essere affidabili e fedeli al sistema.
* I generali non devono essere influenzati e diventare traditori della rete.
* Devono seguire l'algoritmo del sistema.
* Il gruppo di generali deve raggiungere un consenso o una decisione, indipendentemente dalle azioni dei traditori.
* Il sistema o la rete non devono portare a un attacco del 51% in nessun punto dell'azione.

La tolleranza ai guasti bizantina (BFT) è un approccio di consenso che impedisce al sistema di entrare nel problema dei generali bizantini. Significa anche che il sistema dovrebbe rimanere intatto anche se uno dei nodi (o un generale) si guasta. Inoltre, BFT mira a ridurre l'effetto di nodi (o generali) bizantini dannosi sulla rete.

##### Practical Byzantine Fault Tolerance (pBFT)

Nel 1999, Barbara Liskov e Miguel Castro hanno introdotto un algoritmo di consenso Practical Byzantine Fault Tolerance (pBFT), nel tentativo di superare i problemi di bizantinismo. Il loro obiettivo è garantire una replica pratica della macchina a stati bizantini per tollerare nodi maligni o bizantini.

Il pBFT segue un approccio asincrono. Gli aspetti essenziali dell'algoritmo di consenso pBFT sono i seguenti:

* Tutti i nodi sono riuniti in una sequenza.
* Un nodo della rete funge da nodo leader e gli altri sono nodi di riserva.
* Il nodo primario o leader serve la richiesta del cliente. Funziona come moderatore tra il client e i nodi di backup.
* Tutti i nodi sono in grado di comunicare con altri nodi per verificare i nodi onesti e lo fanno consistentemente e senza soluzione di continuità.
* I nodi onesti devono essere in grado di raggiungere un consenso per il prossimo cambiamento globale della rete basato sulla regola della maggioranza.
* Identifica la fonte del messaggio per assicurarsi che sia stato inviato dal mittente corretto.
* Assicura che il messaggio non sia stato modificato o corrotto nel mezzo.

Il PBT dipende fortemente dalla condizione che il numero massimo di nodi maligni o bizantini deve superare un terzo di tutti i nodi della rete. Pertanto, la sicurezza della rete dipende direttamente dal numero totale di nodi onesti. In breve, un sistema pBFT può gestire nodi difettosi o bizantini quando ci sono nodi totali sulla rete.

Di seguito viene descritto il processo dell'algoritmo di consenso pBFT:

* Un client invia una richiesta al nodo leader.
* Il nodo leader invia la richiesta a tutti i nodi di backup.
* Tutti i nodi lavorano sulla richiesta e inviano una risposta al client.
* Il client attende risposte da tutti i nodi con lo stesso risultato.   
  Qui,

Il meccanismo pBFT consiste in 3 fasi:

* Fase di pre-preparazione: Il nodo leader invia un messaggio pre-preparato a ciascun nodo di backup.
* Preparazione: Dopo aver ricevuto il messaggio pre-preparato dal leader, i nodi di backup inviano il messaggio preparato come risposta a tutti gli altri nodi, incluso il leader. Un nodo è considerato preparato solo se ha ricevuto il messaggio pre-preparato dal leader e ha visto un numero di messaggi preparati da altri nodi.
* Impegno: Se i nodi sono preparati, inviano un messaggio di commit. Se un nodo riceve messaggi di commit, esegue la richiesta del client.

Di seguito un’immagine che ne spiega il funzionamento:  


Riferimento: <https://www.naukri.com/learning/articles/byzantine-fault-tolerance-in-blockchain/>

L'intero processo di verifica in un sistema distribuito utilizza il concetto di firma digitale (usando la crittografia a chiave pubblica come spiegato prima). La validità del messaggio e del mittente è garantita da numeri di sequenza e metadati.

Il modello BFT pratico per il consenso della blockchain è stato adattato alle applicazioni pratiche. L'articolo accademico originale alla base del BFT pratico ha anche delineato le particolari carenze, mostrando al contempo i miglioramenti chiave per l'implementazione dell'algoritmo nei sistemi reali. La Practical Byzantine Fault Tolerance può contribuire a garantire i seguenti vantaggi.

1. Flessibilità e velocità delle transazioni

Prima di tutto, può fornire la garanzia della finalizzazione delle transazioni senza alcun requisito di conferma come nella Proof-of-Work. È possibile riscontrare una notevole differenza tra il modello PoW utilizzato da Bitcoin e il BFT pratico. Quando i nodi in un modello BFT pratico sono d'accordo su un blocco interessato, il blocco è considerato definitivo. La definitività si basa sul fatto che tutti i nodi onesti sono d'accordo sullo stato del sistema in un determinato momento. La comunicazione tra i nodi onesti aiuta a garantire un accordo credibile sullo stato del sistema.

1. Basso consumo energetico

Il prossimo importante vantaggio di questo algoritmo di tolleranza ai guasti bizantino rispetto al consenso PoW è il ridotto consumo di energia. Il modello Proof-of-Work utilizzato in Bitcoin implica la necessità di un round PoW per ogni blocco. Gradualmente, i minatori della rete Bitcoin aumentano il consumo di energia elettrica, che può superare il consumo annuale di elettricità di piccole nazioni.

* Il BFT pratico non comporta sforzi computazionali intensivi, il che porta a una profonda riduzione del consumo di energia elettrica. Con il BFT pratico, i minatori non devono risolvere algoritmi di hashing PoW per ogni blocco, richiedendo risorse computazionali intensive.
* Tuttavia, il BFT pratico presenta anche alcuni inconvenienti. Ad esempio, il modello BFT pratico è applicabile solo nella sua forma classica. Pertanto, è limitato a gruppi di consenso di piccole dimensioni per evitare i volumi ingombranti di comunicazione necessari tra i nodi (poco scalabile). Inoltre, l'uso delle firme digitali e dei codici di autenticazione del metodo per l'autenticazione dei messaggi può presentare problemi di inefficienza. Di fatto, è suscettibile agli attacchi Sybil di impersonificazione di nodi

##### Delegated Byzantine Fault Tolerance (dBFT)

Delegated Byzantine Fault Tolerance o dBFT è un meccanismo di consenso reso popolare da una criptovaluta chiamata NEO. dBFT funziona essenzialmente in modo simile al sistema di governo di un Paese, con i suoi cittadini, i suoi delegati e i suoi relatori per garantire che il Paese (la rete) sia funzionale. Il metodo è più vicino al PoS che al PoW, in quanto utilizza un sistema di votazione per scegliere i delegati e gli oratori.

* Il dBFT è una variante del classico algoritmo di consenso Byzantine Fault Tolerance (BFT), ma con la caratteristica aggiuntiva che prevede la presenza di nodi rappresentativi (o "delegati") che agiscono come intermediari tra la rete e i partecipanti. Questo si nota essere simile a DPoS (Delegate Proof of Stake)
* A prima vista, il meccanismo di consenso dBFT è simile alla Proof-of-Stake delegata. Utilizzando un processo di votazione, i possessori di token NEO hanno il diritto di votare per i delegati. Questo indipendentemente dalla quantità di valuta in loro possesso.
  + Chiunque può diventare un delegato, purché soddisfi i requisiti richiesti. Ciò significa una connessione internet affidabile, l'attrezzatura giusta, un'identità convalidata e 1.000 GAS (token usato all’interno della rete NEO). Il GAS è la ricompensa che gli utenti ricevono per la loro attività sulla rete. Tra i delegati viene scelto a caso un oratore.
  + L'oratore costruisce un nuovo blocco dalle transazioni che attende di essere convalidato. Quindi, l'oratore invia la proposta ai delegati eletti. Questi ultimi devono tenere traccia di tutte le transazioni e registrarle sulla rete.
  + I delegati sono liberi di condividere e confrontare la proposta ricevuta per verificare l'accuratezza dei dati e l'onestà dell'oratore. Il blocco viene aggiunto alla blockchain se più di due terzi dei delegati raggiungono un consenso e lo convalidano. La votazione nella rete NEO è un processo che avviene in tempo reale.
  + Ciò significa che il titolare di un token NEO può sostenere uno specifico "bookkeeper" attraverso una votazione. Il gruppo selezionato di bookkeeper utilizza quindi il meccanismo di tolleranza ai guasti bizantina per raggiungere un consenso e generare altri blocchi.
  + Uno dei punti di forza dell'utilizzo del meccanismo dBFT consiste nell'assoluta definitività. Dopo la conferma finale, un blocco non può essere biforcato, quindi la transazione non può essere revocata o annullata. Si tratta però di un'arma a doppio taglio.
    - La definitività è in qualche modo garantita dal fatto che NEO non è una rete completamente decentralizzata. Nonostante gli sforzi di NEO per andare in questa direzione, attualmente ci sono solo sette nodi e alcuni delegati che operano sulla blockchain. La maggior parte di questi è collegata al consiglio di NEO.
  + Poiché tutti i delegati possono verificare la proposta di blocco, è facile capire se i dati inviati dall'oratore sono validi o meno. Quindi, se l'oratore è disonesto e invia proposte non valide a due terzi dei delegati, i blocchi non corrisponderanno e i proprietari dei nodi non li convalideranno. Il consenso viene raggiunto con i due terzi dei voti e viene selezionato un nuovo oratore.
  + Se uno dei nodi è corrotto, gli altri delegati possono determinare la validità della proposta confrontando le proprie versioni della proposta. Il consenso può ancora essere raggiunto, poiché sono necessari solo i due terzi dei delegati per convalidare il blocco e sostituire il delegato disonesto.
  + Utilizzando l'algoritmo Delegated Byzantine Fault Tolerance, il consenso può essere raggiunto anche quando sia il relatore che un delegato sono disonesti. Quando si confrontano i blocchi, i delegati possono vedere se l'oratore o un delegato è corrotto e possono concordare di invalidare il blocco, il che porta automaticamente alla selezione di un nuovo oratore.
  + In una di queste tre situazioni, i delegati disonesti devono controllare due terzi della rete per corrompere i dati scritti sulla blockchain. Questo obiettivo è difficile da raggiungere poiché tutti i possessori di token NEO possono votare, i delegati non sono anonimi e diventare proprietario di un nodo costa 1.000 GAS.
* A livello pratico, generare un nuovo blocco sulla catena impiega tra i 15 e i 20 secondi e si raggiunge un throughput (quantità) di transazioni vicino a 1000 TPS (Transaction Per Second). Non si spende energia e le transazioni sono definitivamente concluse dopo la conferma. Come detto, nel caso della blockchain NEO non si possono avere fork.
* Per contro, poiché i delegati devono operare con identità reali per essere eletti, non c'è anonimato sulla blockchain. Il meccanismo richiede blockchain regolamentate, che includono un certo livello di centralizzazione (esattamente ciò che blockchain come Bitcoin ed Ethereum stanno cercando di ottenere).

#### Proof-of-Elapsed-Time (PoET)

La prova del tempo trascorso (PoET) è una tecnica di consenso della rete blockchain che utilizza un sistema di lotteria equo per mantenere l'efficienza del processo evitando un consumo eccessivo di risorse ed energia. Questo algoritmo è stato sviluppato nel 2016 da parte di ricercatori di Intel utilizzando una tecnologia proprietaria, meglio spiegata nei seguenti punti.

* Su una rete blockchain, l'algoritmo decide chi può estrarre monete e chi vince un blocco utilizzando una quantità di tempo generata casualmente. L'algoritmo PoET aumenta la trasparenza garantendo che i risultati della lotteria possano essere verificati da parti esterne eseguendo un codice affidabile in un ambiente sicuro. Tutti i partecipanti hanno la stessa chance di vincere e di aggiungere un nuovo blocco, grazie alla supervisione di un controller. Questo garantisce la fine del periodo di attesa e la creazione di un nuovo blocco, verificando ogni blocco per svegliarlo o meno.

Ci sono due passi principali da considerare:

* Processo di selezione
  + In primo luogo, ogni nodo partecipante deve condividere il proprio certificato tramite Intel Software Guard Extension (SGX), che ne garantisce la validità per generare un nuovo blocco nella rete. Dopodiché, possono ottenere un oggetto timer.
  + I numeri assegnati a ciascun nodo come oggetto timer (tempo di attesa per il conto alla rovescia) dall'istruzione di generazione di numeri casuali di Intel, RAND. Genera numeri casuali difficili da individuare.
  + A questo punto, l'oggetto timer assegnato a ciascun nodo partecipante si attiva.
* Processo di generazione
  + Dopo che l'oggetto temporale termina e il nodo si sveglia, è idoneo a creare un nuovo blocco per la rete.
  + Il nodo attivo genera l'hash (utilizzando una funzione di hash come SHA-256) del suo blocco di transazioni e lo sottopone all'accettazione. Non è necessario che il nodo esegua alcun lavoro di calcolo.
  + Successivamente, l'aggiornamento viene inviato alla rete.

Ci sono alcune implicazioni importanti dell'algoritmo PoET:

* PoET richiede l'utilizzo della tecnologia SGX di Intel, il che significa che solo i computer che supportano SGX possono partecipare alla rete.
* Poiché PoET richiede che i nodi attendano un periodo di tempo casuale prima di poter creare un nuovo blocco, la velocità di creazione dei blocchi può essere influenzata dal numero di nodi nella rete.
* PoET è un algoritmo di consenso energicamente efficiente, poiché non richiede il processo di mining intensivo in termini di energia che è necessario per altri algoritmi di consenso come Proof of Work. In questo modo è veloce e molto scalabile
* Dipende tutta via da tecnologie proprietarie Intel ed è una rete che chiude e condiziona i permessi della rete che la incorpora.

#### Proof of Capacity (PoC)

Proof of Capacity (PoC) è un algoritmo di consenso utilizzato in alcune criptovalute, come Burstcoin. A differenza di altri algoritmi di consenso come Proof of Work (PoW) o Proof of Stake (PoS), PoC si basa sull'uso di spazio su disco invece che sulla potenza computazionale o sulla quantità di monete possedute.

* In breve, Invece di mostrare il tempo di calcolo pesante per estrarre un blocco come in PoW, PoC mostra le operazioni di archiviazione. Richiede ai minatori di fornire la prova della capacità di archiviazione che hanno utilizzato per estrarre un nuovo blocco di transazioni. Il PoC mira a risparmiare la potenza di calcolo per risolvere gli hash crittografici e trovare il nonce appropriato.
* Invece di alterare ripetutamente i numeri nell'intestazione del blocco e di ripetere l'hashing per il valore della soluzione come in un sistema PoW, il PoC funziona memorizzando un elenco di possibili soluzioni sul disco rigido del dispositivo di mining ancora prima che inizi l'attività di mining.

Più grande è il disco rigido, più valori di soluzione possibili possono essere memorizzati sul disco rigido, più possibilità ha un minatore di trovare il valore hash richiesto dal suo elenco, con conseguente aumento delle possibilità di vincere la ricompensa di estrazione.

L’algoritmo funziona in questo modo:

* In primo luogo, il disco rigido viene tracciato: l'elenco di tutti i possibili valori nonce viene creato attraverso l'hashing ripetuto dei dati, compreso l'account di un minatore. Ciascuno di questi nonce contiene 8192 hash, numerati da 0 a 8191. Tutti gli hash sono accoppiati in "scoop", ovvero gli hash adiacenti vengono combinati per formare una coppia di due. Ad esempio, gli hash 0 e 1 costituiscono lo scoop 0, gli hash 2 e 3 costituiscono l'hash 1 e così via.
* La seconda fase prevede l'esercizio di mining vero e proprio, durante il quale un miner calcola un numero di scoop. Ad esempio, se un minatore inizia l'attività di mining e genera uno scoop numero 38, il minatore va allo scoop numero 38 del nonce 1 e utilizza i dati di quello scoop per calcolare un valore di scadenza.
* Il processo si ripete per calcolare la scadenza di ogni nonce presente sul disco rigido del minatore. Dopo aver calcolato tutte le scadenze, il miner seleziona quella con la scadenza minima.

A livello di vantaggi:

* PoC può utilizzare qualsiasi disco rigido normale, compresi quelli con sistemi basati su Android
* Si dice che sia fino a 30 volte più efficiente dal punto di vista energetico rispetto al mining basato su ASIC della criptovaluta bitcoin
* Non è necessario un hardware dedicato o un aggiornamento costante dei dischi rigidi
* I dati di mining possono essere facilmente cancellati e l'unità può essere riutilizzata per qualsiasi altro scopo di archiviazione dati. Inoltre, sono più centralizzati

A livello di svantaggi:

* Non molti sviluppatori hanno adottato questo sistema
* È possibile che il malware influisca sulle attività di mining
* L'adozione diffusa del PoC potrebbe dare il via a una "corsa agli armamenti" per la produzione di dischi rigidi di maggiore capacità

## Tipi di blockchain

Partiamo da una distinzione esterna; le blockchain *permissionless (senza permessi), permissioned (con permessi-autorizzate)* o entrambe. In particolare definiamo che:

* Le permissioned richiedono il permesso di un’autorità centrale per partecipare. Esse limitano l'accesso alla rete a determinati nodi e possono anche limitare i diritti di tali nodi su tale rete. Le identità degli utenti di una blockchain autorizzata sono note agli altri utenti della blockchain autorizzata.
  + Le blockchain autorizzate tendono a essere più efficienti. Poiché l'accesso alla rete è limitato, ci sono meno nodi sulla blockchain, con conseguente riduzione del tempo di elaborazione per ogni transazione.
* Le permissionless non richiedono alcun permesso per partecipare e permettono agli utenti di essere pseudoanonimi (usando uno pseudonimo non si rivela alcun dettaglio relativo all’identità personale) e non restringono i permessi dei nodi.
  + Le blockchain senza permessi tendono a essere più sicure delle blockchain con permessi, perché ci sono molti nodi che convalidano le transazioni e sarebbe difficile per i cattivi attori colludere sulla rete. Tuttavia, le blockchain permissionless tendono anche ad avere lunghi tempi di elaborazione delle transazioni a causa dell'elevato numero di nodi e delle grandi dimensioni delle transazioni.

Chiaramente, la centralizzazione delle blockchain autorizzate a un'autorità centrale (che sia un governo, un'azienda, un gruppo commerciale o un'altra entità o gruppo che concede l'autorizzazione ai nodi e crea le restrizioni della blockchain) rende il sistema meno sicuro e più incline alle tradizionali vulnerabilità di hacking. Meno nodi ci sono su una blockchain, più è facile per i cattivi attori colludere, quindi gli amministratori di blockchain private devono assicurarsi che i nodi che aggiungono e verificano i blocchi siano altamente affidabili.



Riferimento: <https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between>

I tipi di blockchain principali sono 4:

* Blockchain Pubbliche (Public Blockchain), sistema di libro mastro distribuito non restrittivo e privo di permessi. Chiunque abbia accesso a Internet può registrarsi su una piattaforma blockchain per diventare un nodo autorizzato e far parte della rete blockchain.
  + Un nodo o un utente che fa parte della blockchain pubblica è autorizzato ad accedere ai record attuali e passati, a verificare le transazioni o a fare il proof-of-work per un blocco in arrivo e a fare mining.
  + L'uso più semplice delle blockchain pubbliche è il mining e lo scambio di criptovalute. Pertanto, le blockchain pubbliche più comuni sono quelle di Bitcoin e Litecoin.
  + Su queste blockchain pubbliche, i nodi "minano" criptovalute creando blocchi per le transazioni richieste sulla rete risolvendo equazioni crittografiche. In cambio di questo lavoro, i nodi miner guadagnano una piccola quantità di criptovaluta. I minatori agiscono essenzialmente come cassieri di banca della nuova era che formulano una transazione e ricevono (o "minano") un compenso per i loro sforzi.
  + Le blockchain pubbliche sono per lo più sicure se gli utenti seguono rigorosamente le regole e i metodi di sicurezza. Tuttavia, è rischiosa solo quando i partecipanti non seguono scrupolosamente i protocolli di sicurezza.
* A livello di vantaggi:
  + Sono *sicure*, in quanto ci possono essere quanti più partecipanti o nodi; più grande la rete, maggiore la distribuzione di record ed è più difficile per gli hacker colpire l’intera rete. Inoltre, ciascun nodo farà verificata di transazioni e PoW, rendendo ogni transazione e blocco legittimi.
  + Sono *affidabili*, poiché due nodi o partecipanti non devono preoccuparsi dell'autenticità dell'altro. In altre parole, non hanno bisogno di conoscere personalmente o di fidarsi degli altri nodi, poiché il processo di proof-of-work assicura che non vi siano frodi nelle transazioni. Si può quindi fidare ciecamente delle blockchain pubbliche senza sentire il bisogno di fidarsi dei singoli nodi.
  + Sono *aperte* e *trasparenti* a tutti i nodi partecipanti. Una copia dei record della blockchain o del libro mastro digitale è disponibile presso ogni nodo autorizzato. Questo rende l'intero sistema blockchain completamente aperto e trasparente. Nessuno può mostrare una transazione falsa o nascondere una transazione esistente, poiché ogni nodo dispone di una copia aggiornata del database in qualsiasi momento.
* A livello di svantaggi:
  + Hanno meno TPS (transazioni al secondo), dato che è un enorme rete con molti nodi e ciascun nodo che verifica e faccia PoW consuma parecchio
  + Sono meno scalabili, essendo lente nel processing e nel completamento delle transazioni
  + Consumano molta energia, dato che appunto girano su PoW
* Blockchain Private (Private/Managed Blockchain), un tipo di blockchain restrittiva o con permessi, che opera solo in una rete chiusa.
  + In una blockchain privata, l'autorità centrale determina chi può essere un nodo. Inoltre, l'autorità centrale non concede necessariamente a ogni nodo gli stessi diritti di esecuzione delle funzioni. Le blockchain private sono solo parzialmente decentralizzate perché l'accesso pubblico a queste blockchain è limitato.
  + Alcuni esempi di blockchain private sono la rete di scambio di valuta virtuale business-to-business Ripple e Hyperledger, un progetto ombrello di applicazioni blockchain open-source.
  + Le reti blockchain private vengono utilizzate per le votazioni, la gestione della catena di approvvigionamento, l'identità digitale, la proprietà dei beni, ecc.
* A livello di vantaggi:
  + Sono veloci, misurate sempre in TPS, in quanto vi è un numero limitato di nodi e aggiungere nuove transazioni ad un blocco è veloce. Questo velocizza il consenso o il processo di verifica su tutti i nodi, raggiungendo un rate di centinaia/migliaia di TPS al secondo
  + Sono scalabili, in quanto essendo più controllate ne si sceglie la dimensione sulla base degli usi dell’organizzazione; aggiungere nodi, essendo una dimensione controllata, sarà più semplice.
* A livello di svantaggi:
  + Richiede la costruzione di sicurezza (trust-building), in quanto non c’è un libro mastro-open ledger e dunque non è possibile sapere per certo tutti i colleghi
  + Risulta meno sicura, in quanto avendo meno nodi, il rischio di attacco è più alto. Se un nodo dovesse prendere il controllo del sistema di gestione centrale, prenderebbe facilmente il controllo di tutta la rete e dei nodi, abusando dell’informazione presente
  + Sono centralizzate, richiedendo un controllo specifico di identità e accessi (Identity and Access Management [IAM]) per funzionare correttamente, in quanto il sistema ha tutti i permessi di controllo ed amministrativi, gestendo tutti i nodi e quali permessi dare loro, venendo meno ad una delle idee base di blockchain.
* Consortium Blockchain, che è una tipologia semi-decentralizzata e autorizzata in cui più di un'organizzazione gestisce una rete blockchain. Tuttavia, la creazione di consorzi può essere un processo difficile, in quanto richiede la cooperazione tra diverse organizzazioni, che presenta sfide logistiche e potenziali rischi antitrust.
  + Inoltre, alcuni membri delle catene di fornitura potrebbero non avere la tecnologia necessaria né l'infrastruttura per implementare gli strumenti blockchain, mentre quelli che ce l'hanno potrebbero decidere che i costi iniziali sono un prezzo troppo alto da pagare per digitalizzare i propri dati e connettersi agli altri membri della catena di fornitura.
  + La società di software aziendale R3 ha sviluppato una serie di soluzioni consortili blockchain per il settore dei servizi finanziari e non solo.
* Blockchain Ibrida (Hybrid Blockchain), un tipo di blockchain controllata da una singola organizzazione, ma con un livello di supervisione eseguito dalla blockchain pubblica, che è necessaria per eseguire determinate convalide delle transazioni.
  + Utilizza le caratteristiche di entrambi i tipi di blockchain, ovvero può avere un sistema privato basato sui permessi e un sistema pubblico senza permessi. Con questa rete ibrida, gli utenti possono controllare chi può accedere a quali dati memorizzati nella blockchain.
  + Solo una sezione selezionata di dati o record della blockchain può essere resa pubblica, mantenendo il resto riservato nella rete privata. Il sistema ibrido di blockchain è flessibile e consente agli utenti di unire facilmente una blockchain privata a più blockchain pubbliche. Una transazione in una rete privata di una blockchain ibrida viene solitamente verificata all'interno di quella rete.

### Sidechain

* Le Sidechain, che sono delle blockchain che validano dati da altri blocchi ed è interoperabile con la blockchain principale. ­Esse permettono la creazione di nuove criptovalute o token basati su blockchain preesistenti. In pratica, le sidechain sono catene laterali che si collegano alla blockchain principale, ma che operano in modo indipendente da essa, con proprie regole e caratteristiche.



Riferimento: <https://www.coindesk.com/learn/an-introduction-to-sidechains/>

* + Esse esistono in quanto la costruzione sulle blockchain pubbliche potrebbe non gestire bene introduzione di nuove caratteristiche senza il consenso tra tutta la comunità, difficilmente gestendo grandi quantità di dati e la base di codice della catena principale
  + Le sidechain beneficiano della decentralizzazione e della sicurezza della blockchain principale sottostante e mantengono la flessibilità necessaria per risolvere casi d'uso altamente specifici.
  + L'aggiunta e la rimozione di funzionalità su una sidechain non dipende dal consenso della comunità della mainchain, poiché le nuove funzionalità interessano solo gli utenti della sidechain. Inoltre, le nuove funzionalità possono essere aggiunte a registri separati della sidechain, riducendo lo stress sulla mainchain.
* Esse possono essere usato per eseguire applicazione blockchain decentralizzate (dApp). Una tipica implementazione della sidechain crea una transazione sulla prima blockchain (la mainchain) bloccando gli asset, quindi crea una transazione sulla seconda blockchain (la sidechain) e fornisce prove crittografiche alla transazione che gli asset sono stati bloccati correttamente sulla prima blockchain.
* Le sidechain hanno una funzione di trasferimento bidirezionale con la blockchain principale, definita come *2-way peg*, che consente di bloccare un certo quantitativo di asset sulla blockchain principale, che poi vengono "trasferiti" sulla sidechain, dove vengono utilizzati per eseguire transazioni specifiche. Questa mantiene la compatibilità, dato che come detto gli asset rimangono bloccati sulla blockchain principale fino a quando non vengono restituiti. Questa deve assumere che gli attori che vi operano, definiti come *validatori*, stiano agendo onestamente.
* Esse operano in maniera *cross-chain* (*cross-chain interoperability*), che consente a diverse blockchain di comunicare tra loro e di trasferire asset e valori da una blockchain all'altra, senza dover passare attraverso la blockchain principale. Per ottenerla si utilizzano diversi approcci, per esempio l’*atomic swap*, che consente lo scambio diretto di asset tra blockchain diverse senza la necessità di intermediari. In questo modo, anche con cripto diverse, si ha subito uno scambio senza passare per la main chain.
  + Questo utilizzo due sottoprotocolli; uno per le transazioni in avanti (dalla mainchain alla sidechain) e l’altro all’indietro (dalla sidechain alla mainchain). Per il primo si ha *full referencing*, implicando che i blocchi sidechain contengono tutti i riferimento ai blocchi della mainchain. Questi sono normalmente delle hash oppure dei riferimenti tramite Merkle Tree. Ad ogni modo, occorre modificare la logica della mainchain per mantenere i riferimenti. Entrambi i trasferimenti sono asincroni
  + Un altro approccio utilizzato per la cross-chain interoperability è quello del *token wrapping*. In pratica, il token wrapping consente di creare un token rappresentativo di un asset su una blockchain diversa. Ad esempio, un token ERC-20 potrebbe essere creato per rappresentare Bitcoin su una blockchain Ethereum. Questo token potrebbe poi essere utilizzato per eseguire transazioni su Ethereum, ma rimane comunque collegato al Bitcoin reale sulla blockchain principale.
* A livello di vantaggi:
  + *Scalabilità*: Una sidechain può offrire transazioni più veloci e meno costose grazie a molte ottimizzazioni, ad esempio spostando un certo tipo di transazione su un'altra catena il cui protocollo è costruito appositamente per quel tipo di transazione. Questo dovrebbe decongestionare la prima catena, rendendola anch'essa più veloce ed economica. Le catene laterali possono anche utilizzare tecniche più veloci e più efficienti.
  + *Sperimentazione/aggiornamento*: L'aggiornamento di una blockchain consolidata con diversi soggetti interessati può essere difficile. Raggiungere il consenso può essere lento, se non impossibile. Le sidechain consentono di testare e diffondere nuove idee senza un ampio consenso.
  + *Diversificazione e governance*: Gli asset di altre blockchain possono essere resi accessibili a più persone. Applicazioni come i prestiti e i mutui nella DeFi (Decentralized Finance) possono avere accesso ad asset di altre catene. Disaccoppiandosi dalla catena principale, si possono testare anche caratteristiche indipendenti e anche creare token personalizzati
* Un esempio di sidechain è *Plasma*, un framework per la creazione di una sidechain (nota anche come child chain o plasma chain) che interagisce con la blockchain di Ethereum. L'architettura plasma può essere vista come un albero gerarchico di sidechain. Poiché ogni catena laterale opera in modo indipendente ed è parallela alla mainchain e alle altre sidechain, la velocità e l'efficienza sono ottimizzate. Inoltre, ogni sidechain può essere utilizzata per elaborare applicazioni uniche nello stesso ecosistema sicuro. Plasma utilizza il proof-of-stake come meccanismo di consenso invece del proof-of-work per garantire un'esecuzione più rapida delle transazioni.
  + Questa viene spesso utilizzata per i cosiddetti *smart contract*, che sono creati e immessi nella catena principale. Questo smart contract contiene le regole, il tasso di scambio dei token e gli hash di stato della sidechain. Una sidechain invia periodicamente informazioni sullo stato alla blockchain madre.
  + Gli impegni dei blocchi scorrono verso il basso e le uscite possono essere inviate a qualsiasi catena madre, per essere infine impegnate nella blockchain principale. La rete di illuminazione può essere implementata in cima allo strato di plasma (cioè le sidechain) per facilitare le transazioni istantanee.

Immagine che contiene diagramma

Descrizione generata automaticamente

Riferimento: <https://crypto.com/university/what-are-sidechains-scaling-blockchain>

* A livello di svantaggi:
  + *Limitata sicurezza,* perché le sidechain non sono protette dal Layer 1 e dipendono invece dai propri validatori per la sicurezza. Attirare un gran numero di validatori interessati può essere difficile, soprattutto per le catene che non dispongono di gettoni nativi che possono servire da incentivo. Essendo catene più piccole, sono più vulnerabili a potenziali attacchi.
  + *Minore decentralizzazione*, in quanto le sidechain sono considerate più centralizzate delle catene principali. Rispetto alle blockchain principali, si affidano a un numero minore di minatori, rendendo l'elaborazione delle transazioni meno decentralizzata. Ciò solleva questioni di compatibilità con la natura decentralizzata della blockchain.

## Scalabilità nelle blockchain

La scalabilità della blockchain si riferisce alla capacità di una rete blockchain di gestire un numero crescente di transazioni senza sacrificare prestazioni, velocità o sicurezza. Si tratta di un aspetto critico della tecnologia blockchain perché determina il numero di transazioni che possono essere elaborate in un determinato periodo di tempo. Nel corso del tempo si sono cercate varie soluzioni per aumentare il numero di transazioni mantenendo i costi o quantomeno diminuendoli.

I principali fattori che influenzano la scalabilità di un protocollo blockchain per quanto riguarda il throughput delle transazioni sono:

* La dimensione di una singola transazione (byte)
* La dimensione del blocco (byte -> transazioni per blocco)
* Tempo di blocco, l'intervallo in cui vengono creati i blocchi (tempo -> blocchi per unità di tempo -> transazioni per unità di tempo)
* Ritardo di propagazione sulla rete (secondi)

Per aumentare il throughput di una blockchain lineare a livello di protocollo si può diminuire la dimensione delle transazioni stesse o l'intervallo in cui vengono creati i blocchi. Un'altra opzione sarebbe quella di aumentare la dimensione dei blocchi.

* Esiste la proposta Segwit (Segregated Witness), che ha creato un aggiornamento soft fork (cioè, un aggiornamento retrocompatibile) che ha permesso il cambio dei blocchi e delle loro dimensioni; i blocchi vecchi non comprenderanno le regole, ma potranno comunque convalidare blocchi e transazioni. Questa soluzione è stata implementata nel protocollo Bitcoin nel 2017, cercando di aumentare la dimensione massima dei blocchi, allora di 1 MB.
  + Senza SegWit, i dati relativi alla firma possono arrivare a occupare fino al 65% di un blocco. Con SegWit, i dati relativi alla firma vengono rimossi dall'input della transazione. Questo porta le dimensioni effettive del blocco da 1 MB a circa 4 MB.
* Invece di includere le informazioni di transazione (come mittente, destinatario, importo, definito come *scriptSig*) all'interno del blocco, SegWit crea una struttura di dati separata chiamata "Witness", che contiene solo le informazioni di autenticazione delle transazioni. Questo consente di separare le informazioni di autenticazione delle transazioni dalle informazioni di transazione reali, permettendo di ridurre il peso delle transazioni e di aumentare il numero di transazioni che possono essere incluse in un blocco.
* I creatori di Segwit avrebbero potuto lasciare che i blocchi di Segwit fossero grandi o piccoli quanto volevano e Segwit sarebbe stato comunque un soft fork, a patto che i blocchi inviati ai nodi Legacy fossero sempre di 1.000.000 di byte o meno. Una restrizione di 1MB per i blocchi Segwit non aumenterebbe affatto le dimensioni dei blocchi, mentre una restrizione di 1GB per i blocchi Segwit aprirebbe un vettore di attacco molto ovvio. Per limitare i blocchi Segwit, i creatori di Segwit hanno invece ideato una restrizione diversa dalla dimensione.
* I blocchi Segwit sono limitati da qualcosa chiamato Block Weight. Il Block Weight è un nuovo concetto introdotto in Segwit e viene calcolato per ogni transazione. Ogni transazione ha un "peso" che è definito in questo modo:
  + (dimensione della transazione con i dati del testimone rimossi) \* 3 + (dimensione della transazione)
* Le transazioni non-Segwit non hanno dati degli witnesses, quindi il peso di una transazione non-Segwit è esattamente 4 volte la dimensione. Le transazioni Segwit hanno alcuni dati witness, quindi il peso sarà inferiore a 4 volte la dimensione. Si noti che le transazioni Segwit vengono trasmesse ai nodi Legacy senza dati witness, quindi questa formula darà sempre come risultato blocchi comunicati ai nodi Legacy che sono inferiori o uguali a 1.000.000 di byte. Ancora una volta, questo è il motivo per cui Segwit è un soft fork.
* Segwit non solo aumenta la scalabilità della blockchain di Bitcoin, ma offre anche importanti vantaggi in termini di sicurezza. Poiché le informazioni di autenticazione delle transazioni sono separate dalle informazioni di transazione reali, la blockchain diventa più resistente agli attacchi di tipo malevolo come gli attacchi di double-spending. Inoltre, SegWit consente di introdurre nuove funzionalità sulla blockchain di Bitcoin, come le transazioni a pagamento multi-firma.

Un’altra soluzione pensata in questo senso è Blockchain Unlimited, il cui obiettivo è sviluppare soluzioni per aumentare la dimensione massima dei blocchi della blockchain di Bitcoin, attualmente limitata a 1 MB. Blockchain Unlimited propone di aumentare questa dimensione, ad esempio a 2 MB o 8 MB, per permettere alla blockchain di elaborare un maggior numero di transazioni in un dato periodo di tempo. Inoltre, Blockchain Unlimited sostiene che un aumento della dimensione dei blocchi della blockchain di Bitcoin può favorire la decentralizzazione della rete, permettendo a un maggior numero di nodi di partecipare alla validazione delle transazioni.

* Una delle soluzioni proposte da Blockchain Unlimited per aumentare la dimensione dei blocchi della blockchain di Bitcoin è Bitcoin Unlimited, un software alternativo al software ufficiale di Bitcoin che permette di scegliere la dimensione dei blocchi. Con Bitcoin Unlimited, i nodi possono scegliere di elaborare blocchi di qualsiasi dimensione, a patto che almeno il 75% dei nodi aderisca alla stessa dimensione di blocco. Questo sistema, secondo Blockchain Unlimited, permette una maggiore flessibilità e adattabilità della blockchain di Bitcoin, e permette di aumentare la scalabilità della rete.
* Tuttavia, la proposta di Blockchain Unlimited ha incontrato diverse critiche da parte della comunità Bitcoin, soprattutto per quanto riguarda i possibili rischi per la sicurezza della rete e la decentralizzazione della stessa. L'aumento della dimensione dei blocchi della blockchain di Bitcoin potrebbe infatti comportare un maggior rischio di attacchi di tipo malevolo, e potrebbe favorire la centralizzazione della rete, con un maggior potere di controllo dei grandi miner sulla validazione delle transazioni.

Gli approcci alla scalabilità sono generalmente tre:

* *Tecnologie di secondo livello (second layer technologies)*, come i canali di pagamento o di stato utilizzati nella Lightning Network, che portano le transazioni fuori dalla catena con l'opzione di regolare la catena in qualsiasi momento.
* *approcci Sidechain*, che possono essere meglio descritti come una parallelizzazione delle blockchain. Le attività possono essere trasferite da una catena all'altra tramite un peg (cioè, il prezzo specifico a cui punta un token, agganciando il riferimento ad un’altra valuta) bidirezionale (2WP) e il carico transazionale è condiviso tra la mainchain e le sue sidechain.
* I grafi aciclici diretti (DAG) hanno una struttura di dati diversa dalle blockchain. Molti blocchi possono essere prodotti in parallelo, il che richiede modifiche al meccanismo di consenso.

### Immagine che contiene grafico Descrizione generata automaticamenteDirected Acyclic Graphs (DAG)

I grafi aciclici diretti (Directed Acyclic Graphs o DAG) rappresentano una tecnologia alternativa alle blockchain tradizionali, utilizzata per la gestione dei registri digitali distribuiti. A differenza delle blockchain, basate su una struttura lineare a catena di blocchi, le DAG utilizzano una struttura ad albero, in cui i nodi rappresentano le transazioni e i rami rappresentano le connessioni tra le transazioni.

Un grafo aciclico diretto non ammette relazioni cicliche tra i nodi, come quella che si può vedere nella parte a forma di diamante del grafo diretto al centro. In termini tecnici, si direbbe che il grafo G = (V, E) è definito come l'insieme dei vertici V e degli spigoli E.

* In una DAG, ogni transazione viene aggiunta come nodo nella struttura e si connette con i nodi precedenti che hanno influenzato il suo stato. Questo processo di connessione dei nodi forma una rete di transazioni che rappresenta l'intera storia delle transazioni all'interno della DAG. La connessione tra le transazioni viene gestita in modo dinamico, in modo che le transazioni più recenti possano essere validate più velocemente, riducendo i tempi di conferma. La differenza principale è che qui transazioni multiple possono essere riferite, piuttosto che una sola alla volta
* Il DAG introduce la bidimensionalità nella struttura dei dati altrimenti lineare o unidimensionale della blockchain ed è un approccio promettente per rendere scalabili le reti decentralizzate. Rispetto a una blockchain, cambiamo solo la struttura dei dati, ma manteniamo lo stesso meccanismo di consenso, Proof-of-Work, per far sì che la rete si accordi su un'unica cronologia delle transazioni.
* Una delle caratteristiche principali delle DAG è la possibilità di eseguire operazioni di transazione in parallelo, consentendo di elaborare più transazioni contemporaneamente, senza l'attesa di una conferma per la transazione precedente. Questa capacità rende le DAG molto adatte per l'elaborazione di transazioni ad alta velocità, come ad esempio le micro-transazioni.

Esistono vari modi per impostare un DAG da utilizzare per una criptovaluta.

* Scegliere un algoritmo di DAG; di questi ne esistono molteplici:
  + IOTA's Tangle: IOTA è una criptovaluta basata su DAG che utilizza una struttura di dati chiamata Tangle. Nel Tangle, ogni transazione è rappresentata da un nodo e ogni nodo è collegato a due nodi precedenti. Quando viene effettuata una nuova transazione, questa deve convalidare due transazioni precedenti per essere confermata. Questo processo è chiamato "selezione della punta". IOTA si avvale anche di un "Coordinatore" per prevenire alcuni tipi di attacchi e garantire il buon funzionamento della rete.
  + SPECTRE (Shortest Path First Tangle): Essa è una criptovaluta basata su DAG, progettata per risolvere alcuni dei problemi di scalabilità e sicurezza del Tangle. In SPECTRE, ogni transazione è rappresentata da un nodo e i nodi sono collegati tra loro in modo da creare un grafo aciclico diretto. SPECTRE utilizza un meccanismo di consenso chiamato "greedy heaviest observed subtree" (GHOST) per confermare le transazioni e mantenere la rete.
  + Phantom: Essa è una criptovaluta basata su DAG che utilizza una struttura di dati chiamata "unità phantom" per rappresentare le transazioni. L'unità fantasma è una combinazione di due transazioni precedenti ed è collegata ad altre unità fantasma per creare un DAG. Phantom utilizza un meccanismo di consenso chiamato "Casper FFG" (Friendly Finality Gadget) per confermare le transazioni e mantenere la rete.
* Definire la struttura delle transazioni
  + Le criptovalute basate su DAG utilizzano una struttura di transazioni diversa da quella delle blockchain tradizionali. Ogni transazione è rappresentata da un nodo del DAG, collegato ad altri nodi che rappresentano transazioni precedenti. È importante definire la struttura delle transazioni e le regole per collegarle.
* Impostare meccanismo di consenso
* Determinare gli incentivi per i singoli nodi
  + In una criptovaluta basata su DAG, i nodi sono responsabili della conferma delle transazioni e della manutenzione della rete. È importante determinare gli incentivi per i nodi a partecipare alla rete, come le commissioni per le transazioni o le ricompense per i blocchi.
* Sviluppare un wallet e una UI
  + Come le criptovalute tradizionali, le criptovalute basate su DAG richiedono un portafoglio e un'interfaccia utente che permetta agli utenti di interagire con la rete. È importante sviluppare un'interfaccia facile da usare che renda semplice per gli utenti inviare e ricevere transazioni.
* Testare e lanciare

Solo poche criptovalute usano le DAG; di fatto è un modello che abbatte i costi energetici e di transazione legati al mining collegati, in quanto siamo nelle prime fasi di utilizzo; normalmente, vengono usati nella fase di test della rete e non di suo stabile utilizzo.

#### blockDAG

In un blockDAG, le transazioni sono organizzate in blocchi, che vengono poi collegati per formare un DAG. Ciò consente tempi di elaborazione delle transazioni più rapidi e una migliore scalabilità rispetto a una blockchain tradizionale, pur mantenendo la sicurezza e l'affidabilità di una blockchain.

Ecco alcune differenze tra i blockDAG e le blockchain tradizionali:

* Struttura: In una blockchain tradizionale, le transazioni sono raggruppate in blocchi collegati in una catena lineare e cronologica. In un blockDAG, le transazioni sono raggruppate in blocchi collegati in una struttura DAG.
* Consenso: Le blockchain tradizionali utilizzano meccanismi di consenso come Proof of Work o Proof of Stake per convalidare le transazioni e mantenere la rete. I BlockDAG spesso utilizzano una combinazione di meccanismi di consenso per ottenere una migliore scalabilità e sicurezza.
* Biforcazioni: Le biforcazioni possono verificarsi sia nelle blockchain tradizionali che nei blockDAG, ma il modo in cui vengono risolte è diverso. In una blockchain tradizionale, i fork vengono risolti scegliendo la catena più lunga. In un blockDAG, le biforcazioni possono essere risolte scegliendo il ramo più pesante, che tiene conto sia della lunghezza che del peso di ciascun ramo.

Immagine che contiene diagramma

Descrizione generata automaticamente

Riferimento: <https://ancapalex.medium.com/an-introduction-to-the-blockdag-paradigm-50027f44facb>

* In un libro mastro blockDAG, i nuovi blocchi fanno riferimento a tutte le punte del grafo (blocchi che non sono ancora stati referenziati) che i loro minatori vedono localmente. Come in una blockchain, i blocchi vengono pubblicati immediatamente.
* Tuttavia, a differenza di una blockchain che, per costruzione, preserva la coerenza (ogni blocco della catena aggiunge transazioni che sono coerenti con i suoi predecessori nella catena), un blockDAG incorpora blocchi provenienti da diversi "rami" e quindi può contenere molte transazioni in conflitto. Per questo motivo, un DAG, o blockDAG, non può essere considerato una "soluzione" o un "nuovo protocollo" di per sé. Invece, un blockDAG è un quadro di riferimento per l'ideazione di protocolli di consenso che possono essere (o meno) sicuri e più scalabili dei protocolli basati sulle catene.

I protocolli BlockDAG come SPECTRE e PHANTOM evitano i problemi associati agli alti tassi di orfanità. Questo comporta numerosi vantaggi:

* Permette tempi di conferma dell'ordine dei secondi, almeno quando sono visibili doppi pagamenti e conflitti.
* Consente un'ampia velocità di transazione, limitata solo dalla capacità della dorsale di rete e degli endpoint; ciò implica anche commissioni ridotte.
* Contribuisce alla decentralizzazione del mining consentendo circa 100.000 blocchi al giorno, il che riduce l'incentivo a unirsi a un pool di mining.
* Evita il rischio di orfanizzazione, con molti vantaggi aggiuntivi (come la compatibilità con il Layer Two).
* Elimina il selfish mining premiando tutti i blocchi senza discriminare tra blocchi on-chain e off-chain.

# 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/>
* Blog Medium
  + <https://jimmysong.medium.com/>
  + <https://medium.com/coinmonks/>
  + <https://marcomanoppo.medium.com/>
  + <https://ancapalex.medium.com/>
* Canali YouTube:
  + <https://www.youtube.com/@DappUniversity>
* Academy Binance: <https://academy.binance.com/it/articles/>
* Blockchain4Innovation: <https://www.blockchain4innovation.it/>
* QuickNode: <https://www.quicknode.com/>
* Cointelegraph: <https://cointelegraph.com/>
* Affidaty: <https://affidaty.io/blog/it/>
* Bitstamp: <https://www.bitstamp.net/learn/crypto-101/>
* Gemini: <https://www.gemini.com/it-IT/cryptopedia/>
* 101Blockchain: <https://101blockchains.com/>
* Naukri: <https://www.naukri.com/learning/articles/>
* Yahoo Finance: <https://finance.yahoo.com/news/>
* Komodo Academy: <https://komodoplatform.com/en/academy/>
* Hacken.io: <https://hacken.io/insights/>
* Horizen.io: <https://www.horizen.io/academy/>
* AnalyticSteps: <https://www.analyticssteps.com/blogs/>
* Foley: <https://www.foley.com/en/insights/publications>
* Data-Flair: <https://data-flair.training/blogs/>
* Limechain: <https://limechain.tech/blog/>
* WeSecureApp: <https://wesecureapp.com/blog/>
* Tesi di riferimento:
* <https://amslaurea.unibo.it/7934/1/bertani_beatrice_tesi.pdf>
* Libri di riferimento:
  + <https://hacken-3.gitbook.io/l1-security/>
  + <https://tokens-economy.gitbook.io/>