Sommario

[Blockchain: concetti di base 3](#_Toc132652099)

[Blocco 3](#_Toc132652100)

[DLT – Distributed Ledger System 4](#_Toc132652101)

[Fork 4](#_Toc132652102)

[Versioni 5](#_Toc132652103)

[Transazione 7](#_Toc132652104)

[Tipi di transazioni 9](#_Toc132652105)

[Criptovalute 10](#_Toc132652106)

[Tipi principali 10](#_Toc132652107)

[Wallet 16](#_Toc132652108)

[Crittografia nelle blockchain 19](#_Toc132652109)

[Mining dei blocchi 24](#_Toc132652110)

[Perché fare mining 25](#_Toc132652111)

[Come si realizza il mining 26](#_Toc132652112)

[Considerazioni sul mining 27](#_Toc132652113)

[Algoritmi di consenso 27](#_Toc132652114)

[Proof of Work 27](#_Toc132652115)

[Proof of Stake 31](#_Toc132652116)

[Altre tipologie di consenso 35](#_Toc132652117)

[Tipi di blockchain 43](#_Toc132652118)

[Sidechain 46](#_Toc132652119)

[Blockchain trilemma 49](#_Toc132652120)

[Scalabilità 51](#_Toc132652121)

[Soluzioni di scalabilità 71](#_Toc132652122)

[Sicurezza 84](#_Toc132652123)

[Blockchain: concetti avanzati 93](#_Toc132652124)

[Token 94](#_Toc132652125)

[Tipologie di token 96](#_Toc132652126)

[Standard per i token 100](#_Toc132652127)

[Fungible Tokens 105](#_Toc132652128)

[NFT (Non Fungible Tokens) 106](#_Toc132652129)

[Tokenizzazione 110](#_Toc132652130)

[Cosa tokenizzare, tipi e benefici 111](#_Toc132652131)

[Ambiti applicativi 113](#_Toc132652132)

[Come creare un token 115](#_Toc132652133)

[Smart contract 116](#_Toc132652134)

[Come funzionano 120](#_Toc132652135)

[Dove vengono usati 120](#_Toc132652136)

[Tipologie 123](#_Toc132652137)

[Pro e contro 124](#_Toc132652138)

[Considerazioni legali e casi d’uso 125](#_Toc132652139)

[Possibili problemi 126](#_Toc132652140)

[Linguaggi per smart contract: Solidity 132](#_Toc132652141)

[Esempi di codice e passi base 132](#_Toc132652142)

[Solidity in a nutshell 141](#_Toc132652143)

[Framework JavaScript per interazione blockchain 143](#_Toc132652144)

[Ethers.js 143](#_Toc132652145)

[web3.js 152](#_Toc132652146)

[Vulnerabilità di Solidity e degli smart contract 168](#_Toc132652147)

[Self Sovereign Identity 180](#_Toc132652148)

[Principi base 181](#_Toc132652149)

[Componenti dell’architettura 182](#_Toc132652150)

[Settori applicativi 188](#_Toc132652151)

[Protocolli 192](#_Toc132652152)

[Casi d’uso reali 199](#_Toc132652153)

[Zero Knowledge Proof 204](#_Toc132652154)

[Esempi 205](#_Toc132652155)

[Tipi 205](#_Toc132652156)

[Consorzi internazionali coinvolti e finanziamenti europei 208](#_Toc132652157)

[Architettura e soluzioni 209](#_Toc132652158)

[Casi d’uso reali 220](#_Toc132652159)

[Applicazione alla SSI 223](#_Toc132652160)

[Appunti interni tutor 226](#_Toc132652161)

[Riferimenti usati 227](#_Toc132652162)

# 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. Definiamo alcune caratteristiche di base:

* 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.

## Blocco

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.

## DLT – Distributed Ledger System

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.

## Fork

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).
  + Alcune blockchain vengono create per testare funzionalità e non creare overhead sulla rete principale, permettendo di testare nuove caratteristiche prima che ne venga fatto il deploy sulla rete principale, chiamate *testnet*.

## Versioni

La tecnologia blockchain ha avuto tre iterazioni fondamentali nel corso degli anni. Per essere chiari, considereremo la prima iterazione come la versione concettualizzata e implementata dal gruppo Nakamoto. Ogni versione successiva della blockchain include ulteriori caratteristiche di codifica e strutturali che consentono agli utenti di eseguire una gamma più ampia di operazioni.

* Versione 1.0: Origine della blockchain moderna: Currency (Valuta)
  + Blockchain 1.0 è stata la prima applicazione della tecnologia implementata da Satoshi Nakamoto, creatore di Bitcoin. Questa versione è la forma più semplice di un libro mastro decentralizzato per la registrazione delle transazioni e l'archiviazione dei dati su diversi computer. In parole povere, le informazioni registrate nelle prime forme di blockchain erano limitate ai valori di un "oggetto" che cambiava proprietà nel tempo. Nella maggior parte dei casi, il "bene" a cui ci riferiamo era una valuta digitale.
  + Questa versione di Bitcoin è essenzialmente un sistema di trasferimento di denaro elettronico che è automatizzato e funziona senza la necessità di un intervento umano tra le transazioni come autorità di fiducia. Questo sistema consente agli utenti di scambiare valute senza l'intervento di una banca (del settore privato o governativo). Il sistema ha permesso agli utenti finali di trasferire fondi in modo anonimo utilizzando portafogli e dando accesso al registro completo delle transazioni a tutti coloro che sono collegati alla blockchain. Era effettivamente trasparente.
  + La tecnologia iniziale consentiva anche ai minatori (utenti che aiutavano a verificare le transazioni eseguendo compiti crittografici attraverso i loro computer) di ottenere ricompense attraverso i meccanismi di Proof of Work integrati nei protocolli.
* Versione 2.0: Smart Contract
  + Il successivo sviluppo della tecnologia blockchain ha ampliato le capacità dei protocolli blockchain. Quattro anni dopo l'ascesa del Bitcoin, Vitalik Buterin ha introdotto il concetto di Ethereum, una tecnologia basata sulla blockchain con alcuni notevoli miglioramenti rispetto alla generazione precedente.
  + Ethereum è stata la prima blockchain con lo smart contract integrato nel suo protocollo. In parole povere, gli smart contract sono un insieme di codici che vengono automatizzati quando si verificano determinate condizioni. Questi contratti consentono a due utenti o organizzazioni di effettuare più di semplici transazioni di criptovaluta. In questo modo, gli accordi tra due parti eseguono automaticamente task complessi e si ha l’utilizzo di applicazioni decentralizzate che hanno permesso la crescita di organizzazioni autonome (DAO)
* Versione 3.0: DApps (applicazioni decentralizzate)
  + Blockchain 3.0 è il livello successivo della tecnologia blockchain e ha una portata più ampia rispetto alle versioni precedenti. Ha applicazioni in settori diversi dalla finanza e dall'economia e si occupa di sostenibilità, scalabilità, economicità, decentralizzazione e sicurezza. Non si ha ancora una chiara definizione di quest’ultima, ma si intende il contenere un ampio insieme di industrie e applicazioni relative ed incentrare a queste tematiche.
  + Una DApp è simile a un'applicazione tradizionale in quanto può avere un frontend scritto in qualsiasi linguaggio che chiama il backend, e il codice del backend viene eseguito su una rete decentralizzata peer-to-peer. A differenza dei programmi centralizzati che vengono eseguiti su server centralizzati, queste applicazioni utilizzano l'archiviazione e la comunicazione decentralizzata e la maggior parte del loro codice backend viene eseguito su una rete decentralizzata.
  + Essa consente anche l'interoperabilità di diverse reti blockchain in tutto il mondo. Richiede soluzioni innovative per integrare diverse tecnologie, compresi i dispositivi IoT e i circuiti integrati specifici per le applicazioni (ASICS). Blockchain 3.0 utilizza algoritmi DAG e rende popolare il modello proof-of-stake (PoS), che elimina l'uso di dispositivi informatici altamente complessi e riduce il consumo energetico.
* Versione 4.0: Rendere la blockchain utilizzabile nell'industria
  + Con le basi gettate dalle versioni precedenti, per noi Blockchain 4.0 descrive soluzioni e approcci che rendono la tecnologia blockchain utilizzabile per le esigenze aziendali. In particolare alle esigenze dell'Industria 4.0.
  + Industria 4.0 significa in breve automazione, pianificazione delle risorse aziendali e integrazione di diversi sistemi di esecuzione. Tuttavia, questa rivoluzione industriale richiede un grado crescente di fiducia e protezione della privacy: è qui che entra in gioco la blockchain.
  + Quando si aggiunge la blockchain ai sistemi IT si ottiene un'integrazione aziendale che consente processi aziendali cross-system/cross-blockchain, ad esempio macchine che ordinano in modo sicuro e autonomo l'arrivo di parti di ricambio. La gestione della catena di approvvigionamento, i flussi di lavoro di approvazione, le transazioni finanziarie e i pagamenti basati sulle condizioni, la raccolta di dati IoT, la gestione della salute e degli asset sono solo alcuni esempi di aree che possono essere potenziate dalla tecnologia blockchain.
  + Blockchain 4.0 significa rendere Blockchain 3.0 utilizzabile in scenari aziendali reali. Soddisfare le richieste dell'Industria 4.0 facendo sì che le promesse della blockchain diventino realtà.

## 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

## Criptovalute

Le criptovalute sono beni digitali creati e scambiati con tecniche crittografiche, costruite sul sistema blockchain. Formalmente, una criptovaluta è un sistema che soddisfa sei condizioni:

* Il sistema non richiede un'autorità centrale; il suo stato è mantenuto attraverso un consenso distribuito.
* Il sistema mantiene una panoramica delle unità di criptovaluta e della loro proprietà.
* Il sistema definisce se è possibile creare nuove unità di criptovaluta. Se è possibile creare nuove unità di criptovaluta, il sistema definisce le circostanze della loro origine e come determinare la proprietà di queste nuove unità.
* La proprietà delle unità di criptovaluta può essere dimostrata esclusivamente per via crittografica.
* Il sistema consente di effettuare transazioni in cui la proprietà delle unità crittografiche viene modificata. Una dichiarazione di transazione può essere emessa solo da un'entità che dimostri la proprietà attuale di tali unità.
* Se vengono inserite contemporaneamente due diverse istruzioni per la modifica della proprietà delle stesse unità crittografiche, il sistema ne esegue al massimo una.

Esistono molte criptovalute diverse; la tecnologia blockchain è open source, il che significa che qualsiasi sviluppatore di software può utilizzare il codice sorgente originale e creare qualcosa di nuovo con esso. Gli sviluppatori hanno fatto proprio questo. Si stima che al momento della stesura di questo file siano in circolazione più di 10.000 criptovalute diverse, e la cifra continua a crescere.

* Parte della ragione di questa impennata è la relativa facilità con cui è possibile creare nuove criptovalute. Il codice sorgente di una può essere utilizzato per costruirne un'altra. Ad esempio, la rete Ethereum può essere utilizzata per creare monete digitali personali. A volte si verificano dei "fork" nel codice del software che cambiano le regole di funzionamento di una criptovaluta, il che può portare alla creazione di una nuova criptovaluta. Bitcoin Cash (BCH -1,43%) è stato creato nel 2017 come risultato di un fork di Bitcoin che ha permesso di registrare più transazioni su un singolo blocco della blockchain.
* L'impennata dei prezzi delle criptovalute ha spinto molti sviluppatori a cercare di ottenere una fetta dell'azione. Inoltre, la tecnologia blockchain ha un'utilità che va oltre le valute digitali. Quindi, anche se alcune criptovalute potrebbero essere una bolla che alla fine scoppierà, la natura decentralizzata della tecnologia e l'ampio campo di applicazione nel mondo del software sono due ragioni per cui esistono così tante criptovalute.

### Tipi principali

Occorre fare subito alcune distinzioni tra i singoli tipi di valute. Esistono infatti:

* 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

#### Bitcoin (BTC)

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.
  + Nonostante le migliaia di concorrenti che sono sorti, il Bitcoin, la criptovaluta originale, rimane il giocatore dominante in termini di utilizzo e valore economico. Nessuna ha finora eguagliato il suo valore e la sua capacità di mercato.
  + Per contro, l'infrastruttura blockchain di Bitcoin inizia a rallentare una volta superata la velocità di sette transazioni al secondo.
  + 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 (ETH)

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.
  + Essa è una blockchain programmabile general-purpose e Turing completa. Il codice si esegue su smart contracts memorizzate nelle blockchain, in cui lo stato consiste nel balance (saldo) degli account e anche dello storage. La memoria permanente registra anche gli effetti delle transazioni eseguite, così come gli eventi emessi.
  + In essa esistono due tipi di profili: *EOA (Externally Owned Account)*, per cui ad ognuno è associata una chiave privata e generano transazioni esterne e i *contract account*, che non possono generare transazioni esterne e la loro logica è controllata dallo smart contract associato. Ciascuna transazione esterna è firmata digitalmente e ognuna è l’unico elemento in grado di innescare una transizione di stato o causare l’esecuzione di uno smart contract.

#### Tether (USDT)

Tether è una stablecoin, ovvero una valuta legata a una valuta fiat (*fiat currency,* anche detta fiat money, è una moneta a corso legale il cui valore è sostenuto dal governo che l'ha emessa. Si differenzia dalla moneta che è sostenuta da un bene fisico che ne stabilisce il valore, come l'oro, non dipendendo in questo modo da eventi economici), in questo caso il dollaro statunitense. L'idea alla base di Tether è quella di combinare i vantaggi di una criptovaluta (come l'assenza di intermediari finanziari) con la stabilità di una moneta emessa da un governo sovrano (rispetto alle fluttuazioni di prezzo selvagge tipiche di molte criptovalute).

* È una valuta trasparente, in quanto aggiorna quotidianamente sul proprio sito web una ripartizione delle riserve detenute.
* È una valuta stabile; questo promuove l'uso delle stablecoin come mezzo di scambio al pari della moneta convenzionale. In termini pratici, le stablecoin hanno reso più facile la speculazione sui mercati delle criptovalute. La loro rapida crescita di popolarità è anche il risultato dell'uso delle stablecoins come garanzia nei protocolli di prestito e di staking della finanza decentralizzata (DeFi).
* Essendo una stablecoin, ogni token Tether è ancorato a un'unità di valuta fiat o di metallo prezioso. Quindi, ad esempio, una singola unità di USD₮ dovrebbe mantenere un prezzo di mercato di un dollaro USA o molto vicino ad esso. Ciò avviene garantendo che ogni stablecoin sia sostenuta al 100% da attività di riserva detenute da Tether.
* Poiché le attività sono principalmente contanti o equivalenti a contanti emessi da emittenti finanziari tradizionali o garantiti da materie prime, le loro stablecoin sono esempi di stablecoin off-chain. Inoltre, tutti i token vengono controllati, essendo valute stabili e possono esserne creati di nuovi solo da Tether

#### Binance Coin (BNB)

Binance Coin è disponibile sulla piattaforma di scambio di criptovalute Binance, insieme ad altre monete digitali disponibili per il trading. Binance Coin può essere utilizzato come tipo di valuta, ma anche come token che possono essere utilizzati per pagare le commissioni sulla borsa di Binance e per alimentare il DEX (scambio decentralizzato) di Binance per la costruzione di app.

* La moneta di Binance inizialmente girava sulla blockchain di Ethereum con lo standard ERC 20, ma da allora è diventata la moneta nativa della catena di Binance. È stata lanciata durante un'offerta iniziale di monete (ICO) nel luglio 2017 e ha un tetto massimo di 200 milioni di token BNB. BNB era inizialmente basato sulla rete Ethereum, ma ora è la valuta nativa della blockchain di Binance, la Binance chain.
* Vengono spesse eseguite operazioni di *burning* delle monete; Sebbene nell'ICO siano stati inizialmente offerti 100 milioni di token Binance, l'offerta totale attuale è inferiore. Ogni trimestre, Binance utilizza un quinto dei suoi profitti per riacquistare e distruggere definitivamente, o "bruciare", le monete Binance detenute nel suo tesoro; Binance ha regolarmente eseguito questi eventi di burning.

Esso è stato creato come token di utilità per le commissioni di trading scontate nel 2017. Da allora, però, il suo utilizzo si è esteso a numerose applicazioni su un ampio numero di piattaforme. Viene utilizzato per pagare le commissioni di transazione su Binance.com, Binance DEX e Binance Chain.

* Può essere utilizzato anche per i pagamenti (su siti come Crypto.com, Monetha e HTC); per prenotare viaggi (su siti come TravelbyBit, Trip.io e Travala.com); per scopi di intrattenimento (regali virtuali, pacchetti di carte, lotterie); per pagare servizi online (BitTorrent, Canva, Storm); e persino per scopi finanziari (per ottenere un prestito su ETHLend o per fare investimenti su Moeda).

Al di là dell'exchange Binance, Binance Coin ha diversi utilizzi, tra cui la possibilità di:

* Effettuare pagamenti con carta di credito
* Pagare l'organizzazione di viaggi (su siti web selezionati)
* Acquistare regali virtuali
* Elaborare pagamenti
* Effettuare investimenti
* Effettuare prestiti e trasferimenti
* Donare in beneficenza

#### USD Coin (USDC)

USD Coin è un'altra stablecoin e, come Tether, è ancorata al dollaro statunitense. Come Tether, anche USD Coin è ospitata sulla blockchain di Ethereum. L'idea alla base di USD Coin è quella di creare un dollaro "completamente digitale", che abbia la stabilità della valuta fiat statunitense ma che non richieda un conto bancario o che il possessore viva in un determinato Paese. Piuttosto che un investimento, USD Coin è concepito come denaro di uso quotidiano che può essere speso presso i commercianti su Internet.

#### Cardano (ADA)

Charles Hoskinson, il cofondatore di Ethereum, ha iniziato lo sviluppo di Cardano nel 2015 e ha lanciato la piattaforma nel 2017.

Cardano si è posizionata come alternativa a Ethereum. Entrambe le piattaforme sono utilizzate per applicazioni simili, come i contratti intelligenti, e hanno l'obiettivo di costruire un sistema connesso e decentralizzato. Essa si considera una versione aggiornata di Ethereum e si è autodefinita una piattaforma di "terza generazione", rispetto alle credenziali di "seconda generazione" di Ethereum.

* La piattaforma Cardano si basa sul protocollo di consenso *Ouroboros*. Ouroboros, creato da Cardano nella sua fase di fondazione, è il primo protocollo proof of stake (PoS) progettato per ridurre il dispendio energetico richiesto dal mining proof of work (PoW). A tal fine, elimina le enormi risorse di calcolo utilizzate dall'algoritmo di proof of work.
* La sua criptovaluta prende il nome da Augusta Ada Lovelace, contessa e matematica inglese del XIX secolo riconosciuta come la prima programmatrice di computer.
* Nel sistema PoS di Cardano, la puntata determina la capacità di un nodo di aprire blocchi sulla blockchain. Lo stake di un nodo è pari alla quantità di Ada che detiene a lungo termine. Una partecipazione è un interesse detenuto da un partecipante al pool, garantito da un Ada dato in pegno. L'Ada dato in pegno non può essere utilizzato o speso dal titolare perché è tenuto come garanzia per un comportamento onesto di convalida. Gli utenti con Ada in pegno ricevono ricompense sotto forma di commissioni di transazione. Le ricompense sono distribuite in base alla quantità di Ada che un utente ha puntato.
  + Gli utenti si uniscono alle staking pools - gruppi di possessori di Ada che hanno impegnato le loro monete - e lavorano insieme per aggiornare il libro mastro, aprire nuovi blocchi e guadagnare ricompense.
* Cardano ha implementato il supporto per gli smart contract nel 2021 con l'aggiornamento Alonzo.

Questo aggiornamento della testnet è stata la prima iterazione per portare agli utenti la scalabilità e i casi d'uso promessi. Questo aggiornamento ha permesso agli utenti di creare contratti intelligenti e token non fungibili (NFT) e di gestire più asset. Le versioni future e i fork porteranno i contratti intelligenti e altre funzionalità nella mainnet.

#### Solana (SOL)

Solana è una piattaforma blockchain progettata per ospitare applicazioni decentralizzate e scalabili. Fondata nel 2017, è un progetto open-source attualmente gestito dalla Solana Foundation con sede a Ginevra, mentre la blockchain è stata costruita da Solana Labs con sede a San Francisco.

Solana è molto più veloce in termini di numero di transazioni che può elaborare e ha commissioni di transazione significativamente più basse rispetto alle blockchain rivali come Ethereum.

* Anatoly Yakovenko, cofondatore di Solana, ha pubblicato nel novembre 2017 un white paper che descrive il concetto di proof-of-history (PoH). La PoH è una prova per verificare l'ordine e il passaggio di tempo tra gli eventi, ed è utilizzata per codificare il passaggio di tempo senza fiducia in un libro mastro.
* Nel white paper, Yakovenko osserva che le blockchain allora pubblicamente disponibili non si basavano sul tempo, con ogni nodo della rete che si basava sul proprio orologio locale senza conoscere gli orologi degli altri partecipanti alla rete. La mancanza di una fonte affidabile di tempo (cioè di un orologio standardizzato) significava che quando si usava il timestamp di un messaggio per accettarlo o rifiutarlo, non c'era alcuna garanzia che ogni altro partecipante alla rete avrebbe fatto la stessa identica scelta.
* L'architettura di Solana mira a dimostrare una serie di algoritmi software che eliminano il software come collo di bottiglia delle prestazioni quando viene combinato con una blockchain. La combinazione consente al throughput delle transazioni di scalare proporzionalmente alla larghezza di banda della rete.
  + Essa soddisfa tutti e tre gli attributi desiderabili per una blockchain: è scalabile, sicura e decentralizzata. La sua architettura descrive un limite superiore teorico di 710.000 TPS su una rete gigabit standard e 28,4 milioni di TPS su una rete da 40 gigabit.
* La blockchain di Solana opera su un modello di consenso sia proof-of-history (PoH) che proof-of-stake (PoS). PoS consente ai validatori (coloro che convalidano le transazioni aggiunte al libro mastro della blockchain) di verificare le transazioni in base al numero di monete o token in loro possesso; PoH permette a queste transazioni di essere marcate a tempo e verificate molto rapidamente. Essa rimane molto veloce, avendo sempre la modalità di consenso PoS, supportando gli smart contract e processando decine di migliaia di transazioni al secondo

#### Polkadot (DOT)

Diversi progetti blockchain negli ultimi anni si sono concentrati meno su applicazioni specifiche e più su miglioramenti generali legati all'infrastruttura. Tra questi c'è Polkadot (DOT), probabilmente uno dei progetti di maggior successo che lavora per migliorare la tecnologia fondamentale che alimenta le applicazioni decentralizzate (dApp).

* Il protocollo Polkadot cerca di abbattere le barriere tra i vari ecosistemi blockchain, consentendo una comunicazione senza intermediari tra queste reti. Polkadot può essere considerato come una rete di reti, che permette ad architetture blockchain anche molto diverse di interagire tra loro. Lo fa attraverso le parachain, ovvero blockchain specializzate che hanno funzionalità e token propri.

La rete utilizza l'algoritmo di consenso nominato proof-of-stake (PoS) ed è stata ispirata dal protocollo Ouroboros.

Gli esperti del settore e gli sviluppatori elencano tre ostacoli principali che impediscono la crescita della tecnologia blockchain: velocità, scalabilità e sicurezza. La maggior parte delle blockchain di prima generazione, termine alquanto generico, ha apportato miglioramenti incrementali nel corso del tempo, ma rimane inibita da limitazioni tecniche come la scalabilità.

* Questo ha introdotto il concetto delle parachain, che sono essenzialmente blockchain PoS e possono funzionare in modo indipendente, potendo essere completamente personalizzate dal proprietario. Sono focalizzate su applicazioni con funzionalità e logiche di programmazione limitate a sé stesse. Queste catene fungono da livello di governance della rete e sono un meccanismo di gestione.
  + Ciò che lega queste parachains è la catena di relay (relay chain), responsabile della sicurezza, del consenso e dell'interoperabilità della rete condivisa. La catena di relay convalida i dati e ne garantisce la comprensibilità; in altre parole, è responsabile del raggiungimento del consenso e dell'esecuzione delle transazioni.
* Polkadot contiene anche dei ponti, che collegano le blockchain e permettono di trasferire i dati tra di esse. I ponti stabiliscono l'interoperabilità e possono essere utilizzati per connettersi a reti esterne come Bitcoin (BTC) ed Ethereum.
  + Un'altra parte della rete è costituita dai parathread, una versione su scala ridotta dei parachain che funziona secondo un modello a pagamento. È utile per le blockchain che non richiedono una connettività continua alla rete Polkadot.
* Per quanto riguarda il consenso, All'interno del modello di consenso nominato proof-of-stake di Polkadot esistono tre soggetti interessati. Sono i nominatori, i validatori e i collatori:
  + Nominatori: assicurano la catena di relay e selezionano i validatori affidabili.
  + Validatori: sono responsabili dell'imputazione del DOT, della convalida delle prove dei collatori e della partecipazione al consenso.
  + Collatori: richiedono un coinvolgimento minore rispetto ai validatori: sono responsabili di tenere un registro delle transazioni paracadutate valide e di inviarle ai validatori della catena di relay.
* Il token DOT ha un duplice utilizzo: per la partecipazione alla rete per rafforzarne la sicurezza, detta anche bonding, e nel meccanismo di governance.
  + Staking: Come altre blockchain proof-of-stake, il DOT staking incentiva i partecipanti alla rete ad agire onestamente, detenendo il DOT come garanzia per il buon comportamento. Le ricompense vengono assegnate a coloro che puntano i loro DOT.
  + Governance: I titolari di DOT hanno il diritto e la possibilità di partecipare alle votazioni attraverso i referendum, con uno schema di voto ponderato in base alla partecipazione.

## Wallet

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.

Alcuni esempi di wallet utilizzati:

1. Metamask: È un wallet molto popolare che supporta la rete Ethereum e funziona come una estensione del browser web, permettendo agli utenti di interagire con applicazioni decentralizzate (dApps) e di effettuare transazioni sulla blockchain di Ethereum direttamente dal proprio browser. Caratteristiche distintive includono una buona usabilità, una interfaccia intuitiva e la possibilità di importare o esportare le proprie chiavi private.
2. Ledger Nano S: È un hardware wallet che permette di conservare criptovalute offline in un dispositivo fisico sicuro. Questo dispositivo si connette al computer o allo smartphone tramite USB e permette di eseguire transazioni in modo sicuro. Caratteristiche distintive includono la possibilità di conservare più criptovalute, una interfaccia facile da usare e l'alta sicurezza offerta dalla conservazione offline.
3. Trezor: È un altro hardware wallet che permette di conservare criptovalute offline in un dispositivo fisico. A differenza di Ledger Nano S, Trezor ha una schermata OLED per visualizzare le transazioni in tempo reale e verificare l'autenticità delle transazioni. Caratteristiche distintive includono la compatibilità con più criptovalute, l'interfaccia semplice da usare e l'elevata sicurezza offerta dalla conservazione offline.
4. Exodus: È un wallet software che supporta diverse criptovalute tra cui Bitcoin, Ethereum, Litecoin e molti altri. Exodus ha una interfaccia molto accattivante e facile da usare, con grafici e funzioni di analisi per tenere traccia del valore delle proprie criptovalute. Caratteristiche distintive includono la possibilità di scambiare criptovalute all'interno del wallet e la presenza di una funzione di backup automatico.

### 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 (Merkle trees*)*, 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 (questa è la hash di tutte le hash del Merkle tree). 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.
    - Viene definito come *Merkle proof* il processo di attraversamento di un albero Merkle da una foglia alla radice, con l'hashing di ogni livello con il precedente per produrre un hash unico per la struttura dell'albero
    - Le prove di Merkle vengono utilizzate per decidere i seguenti fattori:
      * Se i dati appartengono all'albero di Merkle
      * Per dimostrare in modo conciso la validità dei dati che fanno parte di un insieme di dati senza memorizzare l'intero insieme di dati.
      * Per garantire la validità di un certo insieme di dati inclusi in un insieme di dati più grande senza rivelare né l'insieme completo né il suo sottoinsieme.
    - Assieme a questa struttura, è importante citare che viene usato anche un particolare tipo di albero in Ethereum. Per introdurla, occorre parlare del *trie*. Esso è una struttura dati ad albero usata per memorizzare e cercare array associativi a coppie chiave valore.
      * Introduciamo il trie PATRICIA, che è una variante speciale del trie radix 2 (binario), in cui invece di memorizzare esplicitamente ogni bit di ogni chiave, i nodi memorizzano solo la posizione del primo bit che differenzia due sottoalberi. Esso utilizza nodi compressi per ridurre la quantità di memoria richiesta per la memorizzazione. In un trie PATRICIA, i nodi con un solo figlio vengono fusi con il loro nodo padre e gli archi tra di essi sono etichettati con i caratteri che rappresentano. Questa tecnica di compressione consente di ottenere una struttura di dati più efficiente dal punto di vista dello spazio, pur mantenendo i tempi di ricerca rapidi di un trie standard.
      * Ethereum combina le strutture per realizzare un Merkle Patricia Trie. In Ethereum, ogni nodo dell'albero è referenziato dal suo valore di hash, come un albero di Merkle. L'hash della radice funge da impronta digitale dell'intero insieme di dati da essa rappresentato. Se un valore-chiave viene aggiornato, anche la radice Merkle cambia. Le chiavi di Ethereum sono rappresentate in formato esadecimale, con 16 caratteri possibili (0-9 e A-F).
      * Il Merkle Patricia trie comprende 4 tipi di nodi:
        + null: Un nodo inesistente, rappresentato come una stringa vuota.
        + ramo: Un nodo che ha collegamenti a un massimo di 16 note figlio distinte, corrispondenti a 16 caratteri esadecimali. Ha anche un campo valore.
        + foglia: Un "nodo finale" che contiene la parte finale della chiave e un valore.
        + estensione: Un nodo "scorciatoia" che memorizza una parte della chiave basata su un prefisso comune e un collegamento al nodo successivo.
      * Ethereum utilizza tre strutture trie. Ne vengono usate diverse in quanto dobbiamo gestire dati permanenti come le transazioni in un blocco impegnato e dati temporanei come il saldo del conto che viene aggiornato. Le strutture dati sono richieste per memorizzarli separatamente. In Ethereum, ogni intestazione di blocco memorizza le radici di tre strutture trie: stateRoot, transactionRoot e receiptsRoot.
        + State trie: Lo state trie / world state trie rappresenta una mappatura tra gli indirizzi dei conti e gli stati dei conti. Lo stato del conto comprende il saldo, il nonce, il codeHash e la storageRoot. La storageRoot è la radice di un trie di memorizzazione del conto, che memorizza i dati contrattuali associati a un conto. La chiave è un indirizzo a 160 bit di un conto Ethereum e il valore è lo stato del conto. Il nodo radice dipende da tutti i dati interni e il suo valore di hash funge da identificatore unico per l'intero stato del sistema.
        + I conti Ethereum vengono aggiunti al trie di stato solo dopo che una transazione è stata registrata con successo su quel conto. Il trie dello stato mondiale memorizza alcuni dati temporanei che vengono aggiornati, modificando frequentemente l'hash della radice. StateRoot è l'hash del nodo radice dello state trie, dopo che tutte le transazioni sono state eseguite e impegnate.
        + Transaction trie: viene creato sull'elenco delle transazioni all'interno di un blocco. Il percorso di una specifica transazione nel trie delle transazioni è tracciato in base alla posizione della transazione all'interno del blocco.

Una volta estratta, la posizione di una transazione in un blocco non cambia. Quindi il trie delle transazioni non viene mai aggiornato. Questo è simile alla rappresentazione ad albero di Merkle delle transazioni in Bitcoin e la verifica delle transazioni può essere fatta in modo simile. Il transactionRoot è l'hash del nodo radice del trie della transazione.

* + - * + Receipt trie: la ricevuta registra il risultato della transazione eseguita con successo. Consiste di quattro elementi: codice di stato della transazione, gas cumulativo utilizzato, log della transazione, filtro Bloom (una struttura dati per trovare rapidamente i log).

La chiave è un indice delle transazioni nel blocco e il valore è la ricevuta della transazione. Come il trie delle transazioni, il trie delle ricevute non viene mai aggiornato. Il receiptsRoot è l'hash del nodo radice della struttura trie popolato con le ricevute di ogni transazione nella parte dell'elenco delle transazioni del blocco;

* + 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.

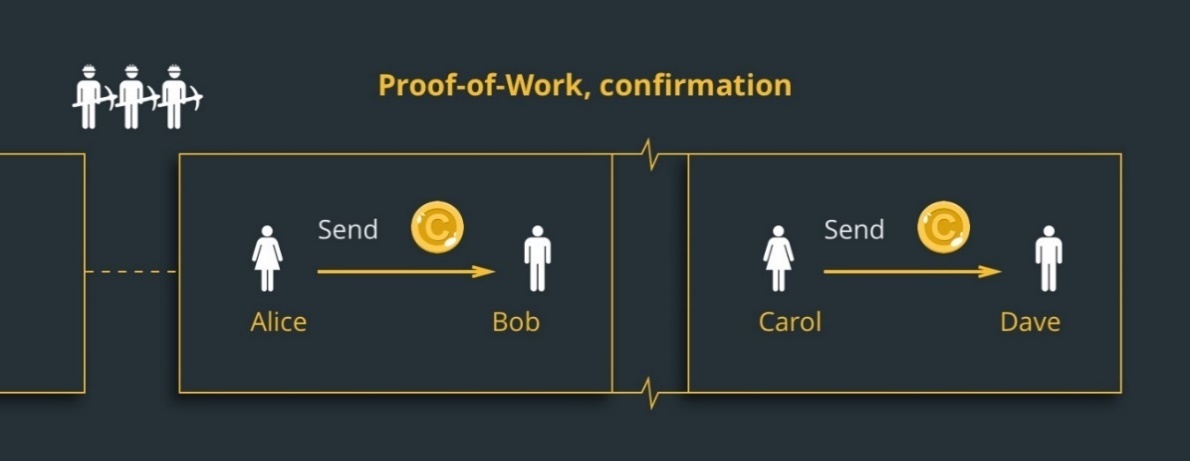
Tuttavia, è importante notare che il consumo di energia associato all'attività di mining non è del tutto dispendioso, in quanto ha un'importante funzione di protezione della rete blockchain e di prevenzione delle frodi. Inoltre, alcuni sostengono che, man mano che le fonti di energia rinnovabile diventano 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

La Leased Proof of Stake 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.

#### Liquid Proof of Stake (LPoS)

Liquid Proof of Stake (LPoS) consente ai titolari di token di prestare i propri diritti di convalida ad altri utenti senza rinunciare alla proprietà del token. Sebbene possa sembrare simile a DPoS, i titolari di token in una rete LPoS scelgono autonomamente se delegare i propri diritti di convalida tokenizzati ad altri utenti o mettere in gioco i propri token. Inoltre, il numero di nodi validatori attivi in LPoS è dinamico, a differenza del numero fisso di validatori di DPoS.

In LPoS, un validatore è chiamato "baker" o "endorser". A differenza del DPoS, ogni utente può diventare un validatore se ha abbastanza monete. Se non ne ha, può scegliere di delegare. L'idea è di diluire ancora di più l'attività e di aumentare l'inclusione. L'attenzione è rivolta più alla liquidità della governance che alla scalabilità della rete. I due ruoli dei delegati sono semplici:

* Creatori: creano blocchi
* Endorser: concordano con i blocchi

Di conseguenza, gli utenti di una rete LPoS hanno un alto grado di flessibilità in termini di partecipazione alla rete. Ad esempio, i grandi possessori di token possono diventare validatori di blocchi puntando i propri fondi senza bisogno di un'approvazione esterna. I piccoli detentori che non hanno le risorse per convalidare da soli i blocchi possono sostenere i detentori più grandi o riunirsi per formare coalizioni efficaci. Allo stesso tempo, poiché i diritti di convalida LPoS sono così fluidi e possono essere facilmente riorganizzati, questa configurazione aiuta a mitigare il rischio che una coalizione di maggioranza prenda il controllo dell'intera rete.

#### Bonded Proof of Stake (BPoS)

Il Bonded Proof of Stake (BPoS) è molto simile all'LPoS: la delega è facoltativa, non vincolante e i detentori di token godono del diritto di voto nelle modifiche del protocollo. Tuttavia, c'è un motivo per cui si chiama BPoS: in caso di errore di sicurezza o di liveness, una parte della partecipazione dei validatori e dei delegatori sarà tagliata. In LPoS, solo il validatore è a rischio di taglio, mentre l'unico rischio dei delegatori è quello di perdere alcune ricompense/interessi nel caso in cui il suo validatore sia disonesto o non efficiente.

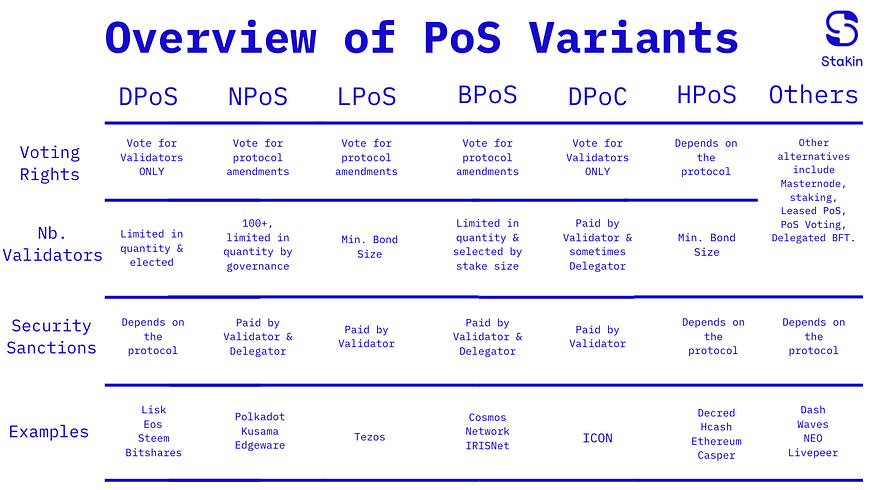
* Questo meccanismo BPoS ha il vantaggio di fornire una soluzione chiara al problema dei rapporti di puntata (simili ai requisiti di capitale) che alcuni validatori dei protocolli LPoS devono mantenere se non vogliono diventare troppo delegati e deludere alcuni dei loro delegatori. Se da un lato risolve questo problema, dall'altro significa che i deleganti devono condurre un approfondimento di informazioni e dati supplementare prima di delegare e rimanere attivi nel verificare le prestazioni del loro validatore.

#### Nominated Proof of Stake (NPoS)

L'ecosistema Polkadot ha introdotto la Nominated Proof-of-Stake (NPoS). In questo sistema, i validatori vengono selezionati automaticamente un paio di volte al giorno. Questi validatori devono eseguire operazioni costose, come garantire un'elevata reattività delle comunicazioni, costruire una reputazione di affidabilità a lungo termine e mettere in gioco il proprio token nativo. Questo viene fatto come garanzia di un buon comportamento e la loro quota viene tagliata ogni volta che si discostano dal loro protocollo.

* In NPoS, i delegatori sono chiamati nominatori. Un nominatore designa i validatori tra un elenco di candidati e blocca una quantità di gettoni di palo con cui sostenerli. In NPoS, il numero di validatori è limitato dalla governance, e questi sono selezionati in base alla loro partecipazione totale nella rete. A differenza dei validatori, un numero illimitato di soggetti può essere nominato. I nominatori sono incentivati a essere sempre alla ricerca di nuovi candidati solidi. Grazie a questi due ruoli, NPoS consente a tutti i titolari di token di partecipare costantemente alla rete. Pertanto, mantiene un elevato livello di sicurezza, pur mantenendo il numero di validatori limitato.

Una piccola overview di tutte le varianti PoS:



Riferimento: <https://medium.com/stakin/proof-of-stake-guide-dpos-vs-lpos-vs-bpos-vs-hybrid-1393a33e849c>

### Altre 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 e 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.

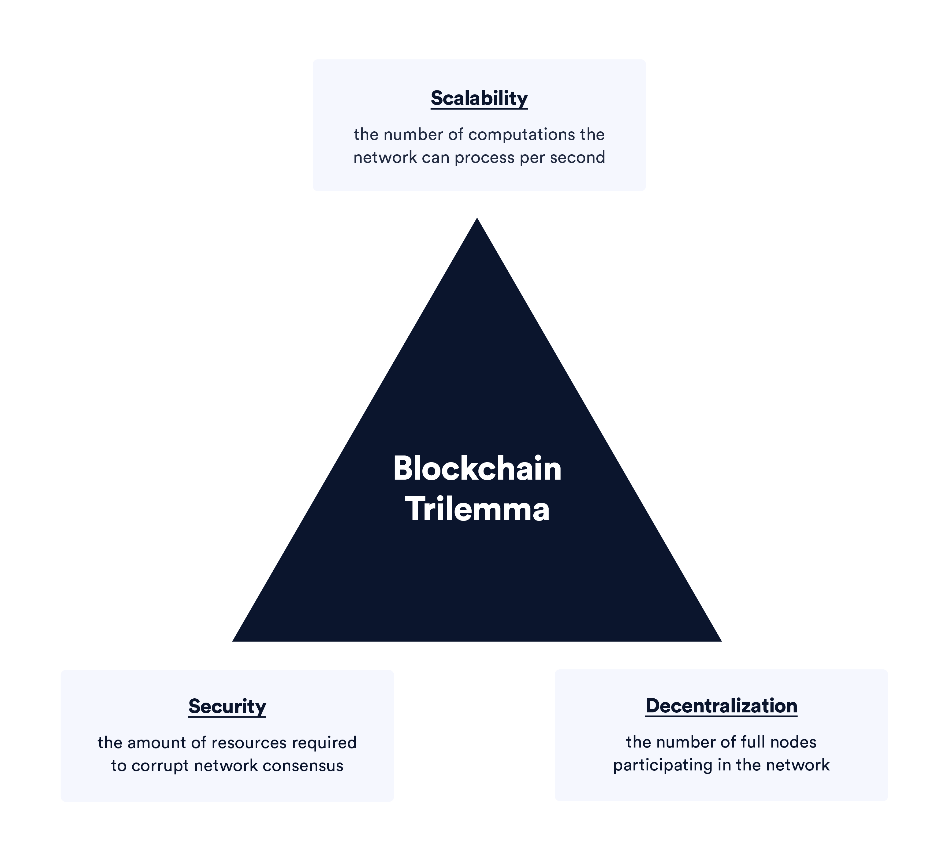
Immagine che contiene diagramma

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.

## Blockchain trilemma



Riferimento: <https://blog.chain.link/blockchain-scalability-approaches/>

Prima di parlare di come scalare le blockchain, è importante capire perché l'informatica delle blockchain è fondamentalmente diversa da quella tradizionale. In generale, le blockchain sono preziose per tre motivi:

* Calcolo deterministico: la logica codificata predefinita viene eseguita esattamente come scritta, con un livello di certezza molto elevato.
* Neutralità credibile: non c'è un amministratore centrale e non ci sono privilegi di rete speciali, il che significa che chiunque può inviare transazioni senza temere censure o discriminazioni.
* Verifica da parte dell'utente finale: lo stato storico e attuale del libro mastro della blockchain e il codice alla base del software client sono verificabili da chiunque nel mondo.

A livello più tecnico, le blockchain hanno il compito di gestire un registro interno di dati, che possono rappresentare la proprietà di beni, lo stato dei contratti o semplicemente informazioni grezze. La maggior parte delle reti blockchain è gestita da due gruppi di partecipanti sovrapposti ma distinti: i produttori di blocchi e i nodi completi.

* I produttori di blocchi raccolgono le transazioni non confermate inviate dagli utenti, ne verificano la validità e le inseriscono in strutture di dati chiamate blocchi. I produttori di blocchi sono generalmente indicati come minatori nelle catene Proof-of-Work (PoW) o validatori nelle catene Proof-of-Stake (PoS), con PoW e PoS che agiscono come meccanismi di resistenza alle sibille per garantire che i libri mastri della blockchain rimangano vivi e immuni alla censura.
* I blocchi inviati dai produttori di blocchi vengono poi accettati o rifiutati dai nodi completi, entità che memorizzano in modo indipendente una copia completa del libro mastro della catena e convalidano continuamente i nuovi blocchi, ma non sono tenuti a partecipare alla produzione dei blocchi. I nodi completi sono gestiti dalla maggior parte dei produttori di blocchi, ma includono anche gli utenti finali e gli attori economici chiave, come le borse, i fornitori di RPC e gli emittenti di stablecoin.
* In definitiva, i nodi completi mantengono l'onestà dei produttori di blocchi rifiutando i blocchi non validi, anche in una situazione in cui la maggior parte dei produttori di blocchi è malintenzionata. Questo rende la creazione di blocchi non validi uno spreco di tempo e denaro, supponendo che esista un numero sufficiente di nodi completi onesti.
* Inoltre, la separazione di tutti i nodi dai produttori di blocchi previene i validatori. Questo fa parte di un sistema di pesi e contrappesi in cui i produttori di blocchi hanno solo il potere di ordinare transazioni, ma non di dettare le regole della blockchain. Le regole sono governate dall'intera comunità dei nodi, alla quale idealmente chiunque può facilmente partecipare.
* Si parla di *trilemma*, perché allo stesso tempo si intende ridurre l’hardware necessario, al fine di abbassare la barriera di ingresso per un interno nodo, che è storicamente il modo in cui le blockchain sono rimaste decentralizzate, una componente critica per generare la minimizzazione della fiducia. Tuttavia, la decentralizzazione è anche la proprietà che generalmente rende le blockchain lente, poiché la rete può operare per lo più solo alla velocità del nodo più lento.
* Di fatto, occorre almeno sacrificare una di queste componenti

#### 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.

### Scalabilità

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)

#### Fattori di scalabilità

La scalabilità della blockchain può essere suddivisa in tre categorie generali.

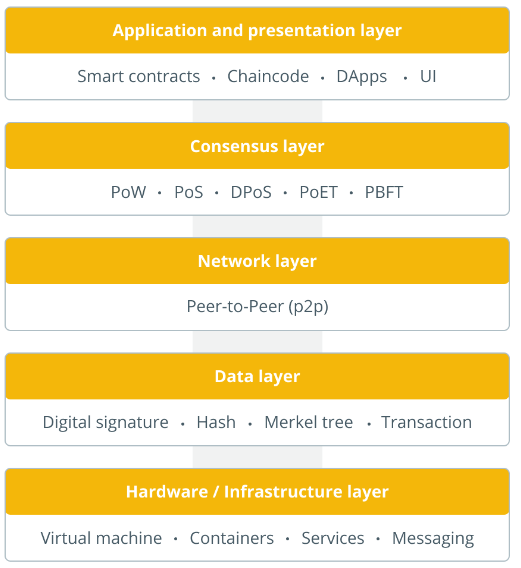
* *Esecuzione*
  + L'esecuzione della blockchain è il calcolo necessario per eseguire le transazioni e i cambiamenti di stato. L'esecuzione delle transazioni comporta il controllo della validità delle transazioni (ad esempio, la verifica delle firme e dei saldi dei token) e l'esecuzione della logica on-chain necessaria per calcolare i cambiamenti di stato. I cambiamenti di stato avvengono quando i nodi completi aggiornano la loro copia del libro mastro per riflettere i nuovi trasferimenti di token, gli aggiornamenti del codice degli smart contract e l'archiviazione dei dati.
  + La scalabilità dell'esecuzione della blockchain è comunemente considerata in termini di transazioni al secondo (TPS), ma a livello più generale si riferisce al numero di calcoli al secondo, poiché le transazioni possono variare in termini di complessità e costo. Più transazioni fluiscono attraverso una rete, più calcoli devono essere eseguiti in un dato momento.
* Quando si scala il livello di esecuzione, il problema principale da risolvere è come ottenere un maggior numero di calcoli al secondo senza aumentare sostanzialmente i requisiti hardware dei singoli nodi completi che convalidano le transazioni in blocchi.
* *Storage* (immagazzinamento)
  + L'archiviazione della blockchain si riferisce ai requisiti di archiviazione dei nodi completi, che mantengono e memorizzano una copia del libro mastro. Le blockchain hanno due forme generali di archiviazione:
    - I dati storici comprendono tutte le transazioni grezze e i dati dei blocchi. I dati delle transazioni comprendono gli indirizzi di origine e di destinazione, l'importo inviato e la firma di ogni singola transazione. I dati dei blocchi comprendono l'elenco delle transazioni e i metadati di un blocco specifico, come la radice Merkle, il nonce, l'hash del blocco precedente, ecc. I dati storici non richiedono in genere un accesso rapido e basta che ci sia almeno un'entità onesta che li renda disponibili per il download.
    - Lo stato globale è un'istantanea di tutti i dati che gli smart contract possono leggere o scrivere, come i saldi dei conti e le variabili all'interno di tutti gli smart contract. Lo stato globale può essere generalmente considerato come il database di una blockchain, necessario per convalidare le transazioni in entrata. Lo stato è comunemente memorizzato all'interno di strutture ad albero (ad esempio gli alberi di Merkle), dove l'accesso e le modifiche possono essere effettuate facilmente e rapidamente da un nodo completo.
  + I nodi completi hanno bisogno di accedere ai dati storici per sincronizzarsi per la prima volta con la blockchain e allo stato globale per convalidare i nuovi blocchi ed eseguire le nuove modifiche allo stato. Man mano che il libro mastro e la memoria associata crescono, il calcolo dello stato diventa più lento e costoso perché i nodi richiedono più tempo e calcoli per leggere e scrivere sullo stato. Se la memoria di un nodo si riempie, dovrà utilizzare lo spazio di archiviazione su disco, il che rallenta ulteriormente la computazione poiché i nodi devono passare da un ambiente di archiviazione all'altro durante l'esecuzione.
* Quando si scala il livello di archiviazione, il problema principale da risolvere è come consentire alle blockchain di elaborare e convalidare un maggior numero di dati senza aumentare i requisiti di archiviazione per i nodi completi; cioè, dove si possono archiviare i dati a lungo termine senza modificare in modo sostanziale i presupposti di fiducia delle blockchain?

* *Consenso*
  + Il consenso della blockchain è il metodo con cui i nodi di una rete decentralizzata raggiungono un accordo sullo stato attuale della blockchain. Il consenso si occupa principalmente di raggiungere una maggioranza onesta di fronte a una certa soglia di attori malintenzionati e di raggiungere la definitività, ossia che le transazioni siano elaborate con precisione e che sia altamente improbabile che vengano annullate. Il consenso della blockchain è generalmente progettato per ridurre al minimo l'overhead di comunicazione, al fine di aumentare il limite superiore della decentralizzazione per una maggiore tolleranza ai guasti bizantini e ridurre il tempo necessario per raggiungere la finalità per una liquidazione più rapida.
* Quando si scala il livello di consenso, il problema principale da risolvere è come raggiungere il risultato finale in modo più veloce, più economico e con una maggiore minimizzazione della fiducia, il tutto in modo prevedibile, stabile e accurato.

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.

#### Blockchain e layers



Riferimento:

<https://cointelegraph.com/learn/a-beginners-guide-to-understanding-the-layers-of-blockchain-technology>

Quando parliamo degli strati della blockchain, è importante notare che ci sono due modi per comprendere la tecnologia blockchain. Possiamo infatti distinguere dei layer a livello fisico e a livello di protocollo

##### Livello fisico

Partendo dal basso:

* Livello di infrastruttura hardware (hardware layer)
  + Il primo livello della blockchain è costituito da hardware, come le connessioni di rete, i computer all'interno della rete e i server di dati. I dati memorizzati all'interno di una blockchain sono ospitati dai server di dati e i computer della rete blockchain possono condividere questi dati tra loro. Questo porta alla creazione di una rete P2P in cui le informazioni vengono convalidate dai singoli nodi (o computer) della rete.
* Livello dati (data layer)
  + In questo livello vengono gestite le informazioni memorizzate sulla rete. Questo livello è costituito da blocchi di informazioni, ogni blocco è collegato al precedente. L'unico blocco che non è collegato a un altro è il blocco genesi (il primo blocco della rete).
  + Ogni transazione scritta su questi blocchi è protetta da una chiave privata e da una chiave pubblica. La chiave privata è una firma digitale conosciuta solo dal proprietario per autorizzare una transazione; la chiave pubblica viene utilizzata per verificare chi ha firmato per la transazione. In parole povere, se qualcuno vi invia una criptovaluta, dovrà conoscere la vostra chiave pubblica; per ricevere la criptovaluta, dovrete usare la vostra chiave privata per verificare la transazione e dimostrare la vostra proprietà al vostro portafoglio blockchain.
* Livello di rete (network layer/propagation layer/P2P layer)
  + Il livello di rete, comunemente chiamato livello P2P, è responsabile della comunicazione tra i nodi. La scoperta, le transazioni e la propagazione dei blocchi sono tutte gestite dal livello di rete. Il livello di propagazione è un altro nome per questo livello.
  + Questo livello P2P garantisce che i nodi possano trovarsi l'un l'altro e interagire, diffondersi e sincronizzarsi per mantenere la rete blockchain in uno stato legittimo. Una rete P2P è una rete di computer in cui i nodi sono distribuiti e condividono il carico di lavoro della rete per raggiungere uno scopo comune. Le transazioni della blockchain sono effettuate dai nodi.
* Livello di consenso (consensus layer)
  + Il livello di consenso è essenziale per l'esistenza delle piattaforme blockchain. Il livello di consenso è il livello più necessario e critico di qualsiasi blockchain, che si tratti di Ethereum, Hyperledger o altro. Il livello di consenso ha il compito di convalidare i blocchi, ordinarli e garantire che tutti siano d'accordo.
  + Gli elementi essenziali di questo livello sono diversi, in quanto questo strato stabilisce un chiaro se di accordi tra i nodi, assicurandosi che la rete resti decentralizzata, che si segua solo una catena stabilendo a quali regole i nodi devono aderire, ottenendo unanimità di accettazione e aiutando ad ottenere affidabilità.
* Livello applicativo (application layer)
  + I contratti intelligenti, i chaincode e le applicazioni decentralizzate (DApp) costituiscono il livello applicativo. I protocolli del livello applicativo sono ulteriormente suddivisi in livello applicativo e livello di esecuzione. Il livello applicativo comprende i programmi che gli utenti finali utilizzano per comunicare con la rete blockchain. Ne fanno parte script, interfacce di programmazione delle applicazioni (API), interfacce utente e framework.
  + La rete blockchain funge da tecnologia back-end per queste applicazioni, che comunicano con essa tramite API. I contratti intelligenti, le regole sottostanti e il codice a catena fanno tutti parte del livello di esecuzione.
  + Anche se una transazione passa dal livello applicativo al livello di esecuzione, viene convalidata ed eseguita nel livello semantico. Le applicazioni danno istruzioni al livello di esecuzione, che esegue le transazioni e garantisce la natura deterministica della blockchain.

###### Scalabilità sull’execution layer

Qui parliamo di scaling verticale, quindi aggiungere più potenza di calcolo ai nodi esistenti, attraverso nuove risorse. Questo migliora i costi, l’efficienza e la manutenzione, ma rende più vulnerabile il tutto a interruzioni e a single point of failure.

L'esecuzione della blockchain può essere scalata aumentando i requisiti hardware dei produttori di blocchi. Requisiti hardware più elevati fanno sì che ogni validatore sia in grado di eseguire più calcoli al secondo.

Da una parte:

* la presenza di un’unica rete decentralizzata composta da validatori porta a blockchain con che possono supportare blocchi più grandi, tempi di blocco più rapidi e costi di transazione più bassi, pur mantenendo la componibilità sulla catena tra gli smart contract e una minimizzazione della fiducia potenzialmente più elevata rispetto ai modelli di calcolo tradizionali.

D’altro canto:

* La scalabilità verticale dei validatori limiterà la decentralizzazione della rete, dato il costo più elevato di gestione di un validatore o di un nodo completo. I costi dei nodi aumenteranno spesso nel tempo, rendendo difficile la partecipazione della maggior parte degli utenti. Il mantenimento della decentralizzazione dipenderà dalla legge di Moore, secondo la quale il numero di transistor su un microchip raddoppia ogni due anni circa, mentre il costo dei computer si dimezza. L'aumento dei costi dei nodi completi può anche aumentare i costi per gli utenti finali che vogliono verificare direttamente le attività che avvengono sulla catena, riducendo la minimizzazione della fiducia.

Ora parliamo di scaling orizzontale, quindi aggiungere nuovi nodi o nuove macchine all’infrastruttura presente. Qui è meglio da un punto di vista di downtime, aumentando la resilienza, performance e tolleranza, richiedendo però più complessità di manutenzione, operazioni e costi iniziali.

Un'alternativa allo scaling verticale è lo scaling orizzontale, attraverso l'uso di più blockchain o sidechain indipendenti all'interno di un singolo ecosistema. Lo scaling orizzontale distribuisce il calcolo delle transazioni in un ecosistema su molte blockchain indipendenti, con ogni catena che ha i propri produttori di blocchi e la propria capacità di esecuzione.

In questo caso parliamo di *scaling vertical con ecosistemi multicatena (multi-chain ecosystems).*

Da una parte:

* Gli ecosistemi multi-catena consentono al livello di esecuzione di ogni singola catena di avere caratteristiche completamente personalizzabili, come i requisiti hardware dei nodi, le caratteristiche di privacy, l'uso dei token di gas, la scelta della macchina virtuale (VM), le impostazioni dei permessi e altro ancora.
* Questo design è il motivo per cui gli ecosistemi multi-catena a volte si traducono in catene di dApp, in cui le singole blockchain si specializzano nel supporto di singole dApp o di piccole collezioni di dApp. Le blockchain auto-sovrane possono anche contribuire a isolare i rischi per la sicurezza, in quanto la scelta di una catena per la sicurezza non influisce sempre sulle altre catene dell'ecosistema.

D’altro canto:

* Gli ecosistemi multi-catena richiedono che ogni blockchain avvii la propria sicurezza attraverso un token nativo emesso in modo inflazionistico. Sebbene questo sia uno standard nelle prime fasi di crescita delle blockchain, potrebbe rivelarsi difficile passare a un modello economico meno diluitivo e più sostenibile, basato sulle tariffe degli utenti della catena, poiché le tariffe degli utenti saranno distribuite su molte blockchain indipendenti. Ci sono anche problemi di componibilità, poiché le dApp e i token che vogliono interoperare non sempre esistono sulla stessa blockchain.

Un altro meccanismo di scaling verticale è lo sharding, implementato all’interno di Ethereum, al fine di garantire il concetto di rete distribuita o trustless e mantenere il throughput. In questo caso, l’aggiornamento è noto come “eth2” sulla rete Ethereum.

Il concetto di sharding consiste nella suddivisione della rete in più sezioni, in grado di operare in maniera parzialmente indipendente, facendo in modo che le sezioni trattino ciascuna operazioni differenti.

Tale meccanismo raddoppia il volume delle transazioni eseguibili, poiché ora il limite è dovuto alla capacità elaborativa dei due nodi in contemporanea. Suddividendo dunque la blockchain in diverse sezioni è possibile aumentare linearmente il numero di operazioni supportate. L’implementazione dello sharding opera sul primo layer del network. Sarà quindi necessario eseguire un fork per aggiornare il protocollo della rete ed inserire le funzionalità di frammentazione.

Lo scopo dello sharding quindi è quello di tagliare i dati e partizionare la rete. La divisione della blockchain di Ethereum consentirebbe a ciascun nodo di memorizzare solo una parte della rete completa, mentre i nodi sarebbero in grado di convalidare la rete attraverso la matematica sottostante e la comunicazione reciproca.

In questo caso si parla di *scaling orizzontale tramite execution sharding*.

Un approccio simile, ma unico, alla scalabilità multi-catena consiste nell'avere una singola blockchain che supporta l'esecuzione parallela su molti shard diversi. Ogni shard agisce essenzialmente come una propria blockchain, il che significa che molte blockchain possono essere eseguite in parallelo. Esiste anche una singola catena principale che ha l'unico scopo di mantenere sincronizzati tutti gli shard.

Nell'execution sharding, c'è un pool di validatori che viene suddiviso tra gli shard per eseguire le transazioni. I nodi vengono ruotati in modo casuale e regolare in modo da non eseguire/convalidare sempre lo stesso shard, con un numero di shard configurato in modo da rendere statisticamente insignificante il rischio di corruzione di un singolo shard.

Da una parte:

* Tutti gli shard di esecuzione attingono dallo stesso pool di nodi, quindi non è necessario eseguire il bootstrap della sicurezza su nuovi shard. Supponendo che ci sia un ampio pool di nodi, ogni ambiente di esecuzione può raggiungere lo stesso livello di sicurezza. Lo sharding dell'esecuzione non richiede inoltre un aumento dei requisiti hardware dei nodi, poiché questi ultimi eseguono l'esecuzione su un solo shard alla volta. Gli shard possono anche operare con la stessa macchina virtuale o utilizzare configurazioni diverse per soddisfare i requisiti unici di alcuni casi d'uso.

D’altro canto:

* Ogni shard ha una flessibilità limitata, dato che tutti i nodi devono essere in grado di supportare la computazione di ogni shard. In genere esiste anche un limite al numero di shard che una blockchain può supportare, a causa dei crescenti requisiti di calcolo richiesti alla catena principale e del rischio di avere un numero troppo basso di nodi per shard. Inoltre, ci sono attriti quando si tratta di bilanciamento del carico e rischi di implementazione, dato che i modelli di sicurezza condivisi significano che tutti gli shard possono essere soggetti alla stessa vulnerabilità.

Un altro approccio di scaling è lo *scaling orizzontale tramite modularità*.

Questo è ottenuto dalle *blockchain modulari*, in cui l'architettura delle blockchain è separata in più livelli diversi, isolando cioè i componenti di esecuzione, disponibilità dei dati (DA) e consenso. Il modo più diffuso di eseguire l'esecuzione nelle implementazioni di blockchain modulari è quello dei rollup, che spostano la computazione e lo stato fuori dalla catena in reti fuori dalla catena, mentre memorizzano i dati delle transazioni nella catena. I cambiamenti di stato calcolati fuori dalla catena sono poi dimostrati proattivamente sulla catena come validi usando prove a conoscenza zero (zk-rollup) o non validi retroattivamente usando prove di frode (optimistic rollup).

Da una parte:

* Le blockchain modulari scaricano l'esecuzione delle transazioni e lo stato su un ambiente di elaborazione più economico, più snello e a più alto rendimento, pur ereditando la sicurezza della blockchain sottostante utilizzata per il regolamento.
* Questo perché il processo di consenso, in cui viene verificata la validità dei calcoli fuori catena eseguiti dal livello di esecuzione, viene eseguito da una blockchain decentralizzata esistente (cioè L1). Intuitivamente, ciò significa che la larghezza di banda computazionale di una blockchain baselayer può essere utilizzata in modo più efficiente perché i nodi completi non hanno bisogno di eseguire ogni transazione. I nodi completi devono solo verificare le prove succinte e memorizzare una piccola quantità di dati delle transazioni.

D’altro canto:

* Le blockchain modulari potrebbero non essere così veloci o economiche come le sidechain o le catene autonome, poiché la maggior parte degli approcci sfrutta l'uso dello spazio di blocco limitato e talvolta costoso di una blockchain baselayer per la sicurezza.
* Gli attuali approcci alle reti modulari comportano anche rischi di aggiornamento che richiedono l'intervento della governance (al di fuori dei rollup immutabili) e possono portare alla frammentazione della liquidità e a problemi di componibilità se alcune dApp rimangono su una blockchain baselayer mentre altre vengono eseguite su diversi livelli di esecuzione off-chain.
* Infine, l'implementazione di un rollup o di altri progetti di blockchain modulari è un processo più nuovo e più complesso rispetto al lancio di una nuova blockchain autonoma.

###### Scalabilità sul data layer

Analogamente al vertical scaling dell'esecuzione della blockchain, il vertical scaling dell'archiviazione della blockchain comporta l'aumento dei requisiti hardware per l'esecuzione di un nodo completo.

Da una parte:

* Le blockchain con limiti di archiviazione più elevati per i nodi completi possono offrire un ampio volume di archiviazione a basso costo, consentendo un accesso più semplice ai dati della catena, non avendo livelli/dipendenze aggiuntive.

D’altro canto:

* Poiché i dati da memorizzare sono sempre più numerosi nel tempo, la decentralizzazione della blockchain diventa sempre più a rischio con l'aumento dei costi di gestione di un nodo completo. Con una minore decentralizzazione, si possono fornire agli utenti meno garanzie di fiducia sulla disponibilità e sulla correttezza dei dati. I blocchi potrebbero inoltre eseguire più lentamente, aumentando la pressione sulla rete.

Un altro approccio per scalare l'archiviazione dei dati delle blockchain è il *data sharding*, effettuato su blockchain di livello 1. Il data sharding suddivide l'archiviazione del libro mastro e/o dei dati utilizzati per ricreare il libro mastro su molti shard, riducendo i requisiti di archiviazione di un singolo nodo in qualsiasi momento a quelli di un singolo shard o di un piccolo insieme di shard.

* Questo permette maggiore decentralizzazione, fornendo inoltre maggiore capacità per memorizzare transazioni; d’altro canto, potrebbero esserci dei limiti al numero di shard una blockchain può supportare, in base al carico della mainchain. È inoltre necessario un campionamento della disponibilità dei dati (DAS), che dimostri che i dati storici necessari per ricostruire una parte del libro mastro erano disponibili in un determinato momento (cioè quando è stato prodotto il blocco) senza che i nodi debbano effettivamente scaricare tutti i dati.

SI parla inoltre di memorizzazione dei dati *in modo compresso con le blockchain modulari*. Le blockchain modulari eseguono i calcoli fuori dalla catena e poi memorizzano i dati delle transazioni o le differenze di stato sia sulla catena che fuori dalla catena. I dati consentono ad altri nodi o utenti di ricostruire lo stato attuale o storico del libro mastro. Quando i rollup utilizzano l'archiviazione dei dati on-chain, i dati delle transazioni sono spesso compressi off-chain prima di essere archiviati on-chain.

* L'archiviazione compressa dei dati sulla catena è la forma più sicura di archiviazione dei dati per le blockchain modulari, perché i dati sono archiviati da tutti i nodi completi della rete. Inoltre, riduce il costo dell'archiviazione dei dati sulla blockchain di livello 1.
* La disponibilità di storage on-chain è più costosa rispetto allo storage off-chain, il che potrebbe inibire la capacità delle blockchain modulari di eguagliare la scalabilità di opzioni di storage meno decentralizzate. La compressione dei dati può anche eliminare parti dei dati non strettamente necessarie per la convalida, inibendo potenzialmente un'analisi più granulare dell'attività della catena basata su tali dati.

Possiamo inoltre avere il *data pruning*, tecnica che consente ai nodi completi della blockchain di scartare i dati storici oltre una specifica altezza di blocco. La potatura dei dati è spesso abbinata ai checkpoint Proof-of-Stake, in cui le transazioni nei blocchi oltre il checkpoint sono considerate definitive, cioè non possono essere annullate senza un grande consenso sociale o un hard fork.

* Il data pruning riduce la quantità di dati che un nodo deve memorizzare o a cui fare riferimento quando partecipa al consenso: il libro mastro è più piccolo perché i dati storici sono già stati convalidati e quindi è sicuro che vengano eliminati. Poiché i dati storici sono già stati convalidati, non sono più necessari se l'intento di un nodo completo è solo quello di convalidare i blocchi futuri, invece di offrire anche uno sguardo storico.
* Tuttavia, la potatura dei dati si basa su terze parti (ad esempio, borse, esploratori di blocchi, ecc.) per memorizzare i dati storici in modo permanente al fine di ricostruire lo stato fino al blocco genesi.
  + Si tratta di un modello di fiducia 1-ad-n, quindi solo una terza parte deve memorizzare i dati in modo onesto affinché un nodo completo sia in grado di ricreare tutto lo stato storico. Con Proof-of-Stake che offre checkpoint e una debole soggettività, questa ipotesi diventa meno rilevante. Tuttavia, tali dati sono ancora importanti per l'analisi della catena e per gli esploratori di blocchi.

Esistono anche metodi incentrati sulla limitazione della quantità di stato che i nodi completi devono memorizzare, in particolare attraverso la scadenza dello stato, la statelessness o le implementazioni di state rent.

* I progetti di scadenza dello stato (state expiry designs) consentono ai nodi di eliminare lo stato a cui non si è acceduto per un certo periodo di tempo, ma utilizzano un tipo di prova di merkle (chiamata "testimone") per far rivivere lo stato scaduto, se necessario.
* I progetti *stateless* sono quelli in cui i nodi completi non sono tenuti a memorizzare lo stato. I nodi completi devono solo convalidare i nuovi blocchi con l'inclusione di testimoni. La statelessness debole si ha quando solo i produttori di blocchi sono tenuti a memorizzare lo stato globale, mentre tutti gli altri nodi possono verificare i blocchi senza memorizzare lo stato.
* I progetti di affitto dello stato (*state rent*) richiedono che gli utenti paghino per mantenere un'archiviazione limitata dello stato. Lo stato che non viene più pagato viene riciclato e affittato a nuovi utenti.

I metodi per limitare i requisiti di memorizzazione dello stato aiutano a limitare la quantità di stato che i singoli nodi devono memorizzare. Ciò contribuisce ad alleviare il gonfiore dello stato, anche in presenza di un libro mastro in crescita o di un numero crescente di transazioni sulla catena. La limitazione della memorizzazione dello stato è fondamentale per mantenere la verifica a lungo termine da parte dell'utente finale, pur mantenendo requisiti hardware pratici.

* Tuttavia, La limitazione dell'archiviazione dello stato è un approccio piuttosto nuovo ed elimina l'idea che gli utenti paghino una sola volta per far sì che ogni singolo nodo completo della rete memorizzi il proprio stato in perpetuo, in netto contrasto con il modo in cui le blockchain gestiscono lo stato oggi.
* Inoltre, l'aggiornamento di una blockchain che utilizza un modello di memorizzazione dello stato tradizionale a un modello di memorizzazione dello stato più limitato è difficile e può rompere le applicazioni che durante lo sviluppo hanno fatto ipotesi specifiche sul fatto che lo stato sia sempre accessibile. I nuovi modelli di memorizzazione dello stato possono anche rendere determinate applicazioni più costose di quanto non fossero in precedenza.

###### Scalabilità sul consensus layer

Di seguito sono riportati quattro obiettivi generali quando si cerca di scalare i meccanismi di consenso della blockchain, che riguardano una maggiore frequenza dei blocchi, una maggiore velocità di finalizzazione e una maggiore robustezza contro i tempi di inattività o gli attacchi malevoli. Si noti che la scalabilità del consenso non riguarda solo la velocità, ma anche l'accuratezza, la stabilità e la sicurezza.

* Aumentare la capacità di esecuzione e di memorizzazione
  + Ciò consentirà a un maggior numero di nodi di partecipare al consenso o almeno impedirà ai nodi esistenti di abbandonare la rete man mano che il libro mastro cresce, contribuendo a mantenere forti garanzie di consenso in termini di tempo di attività, resistenza alla censura, accuratezza e sicurezza.
  + Se la capacità di esecuzione e di archiviazione viene aumentata a un livello significativo senza un impatto significativo sui nodi completi, le blockchain potrebbero persino essere in grado di supportare tempi di blocco più rapidi e/o dimensioni di blocco più grandi in modo stabile senza sacrificare la loro proprietà fondamentale di decentralizzazione.
* Ridurre la larghezza di banda della rete
  + Un altro modo di affrontare la scalabilità del meccanismo di consenso di una blockchain è quello di ridurre la larghezza di banda di rete, cioè l'overhead di comunicazione (invio e ricezione di messaggi) richiesto tra i nodi completi per raggiungere il consenso.
  + Invece di richiedere che i nodi siano in grado di comunicare tra tutti gli altri nodi (cioè il voto da tutti a tutti), il consenso delle blockchain può essere progettato in modo che i nodi debbano comunicare solo con una piccola parte degli altri nodi in qualsiasi momento (ad esempio, il sottocampionamento).
  + Alcuni progetti di consenso non utilizzano schemi di voto o di comunicazione a più turni, in modo che l'unica comunicazione richiesta sia la propagazione dei blocchi, ma questo generalmente va a scapito della finalità probabilistica.
* Aumentare la latenza della rete
  + Esistono anche metodi che cercano di ridurre la latenza della rete durante il consenso, in particolare per quanto riguarda l'abbassamento del tempo di finalizzazione. Alcuni meccanismi di consenso delle blockchain hanno una finalizzazione istantanea, sia attraverso un sottocampionamento a più turni, sia attraverso turni di voto "tutti contro tutti".
  + Altre blockchain implementano checkpoint garantiti da un consenso alla grande maggioranza dei validatori dopo un certo periodo di tempo, il che significa che i blocchi sono considerati definitivi dopo il checkpoint, poiché non possono più esserci riorganizzazioni in-protocollo al di là di esso. Spesso è necessario trovare un compromesso tra latenza e larghezza di banda della rete.
* Aumentare il budget per la sicurezza
  + La minimizzazione della fiducia del consenso può essere scalata anche aumentando il budget di sicurezza che finanzia i nodi che partecipano al consenso. In genere, ciò avviene ottenendo un premio monetario, con ricompense in token inflazionate, e/o aumentando i ricavi delle commissioni di transazione dato che la domanda di spazio per i blocchi supera l'offerta.
  + Budget di sicurezza più elevati aprono maggiori entrate potenziali per i partecipanti, che possono quindi aumentare la decentralizzazione della rete, poiché più nodi sono incentivati a partecipare. Le blockchain possono anche richiedere ai nodi di mettere a disposizione una maggiore partecipazione o potenza di calcolo per partecipare al consenso, anche se questo rischia di aumentare la centralizzazione della rete se i requisiti diventano troppo elevati.

##### Livello logico (protocolli)

Possiamo distinguere 4 tipi principali di layer, partendo dal:

* Layer 0, che è la blockchain stessa. I componenti necessari per rendere reale la blockchain sono internet, l'hardware e molte altre connessioni. La blockchain di livello zero è lo stadio iniziale della blockchain che permette a varie reti di funzionare, come Bitcoin, Ethereum e molte altre. Il livello 0 fornisce inoltre alla blockchain una struttura di comunicazione interoperabile tra le catene dall'alto verso i diversi livelli. Il livello 0 fornisce l'infrastruttura di base della blockchain.
* Layer 1, che è il livello di base e la cui sicurezza si basa sulla sua immutabilità. La rete Ethereum, o primo livello, è ciò a cui si allude quando si parla di Ethereum. Questo livello è responsabile dei processi di consenso, dei linguaggi di programmazione, della durata dei blocchi, della risoluzione delle controversie e delle regole e dei parametri che mantengono la funzionalità di base di una rete blockchain. È anche noto come livello di implementazione. Bitcoin è un esempio di blockchain di primo livello.
* Layer 2, noto anche come livello di esecuzione. Quando una blockchain cresce, aumenta il numero di transazioni eseguite su di essa. Per supportare l'aumento del numero di transazioni, abbiamo bisogno di soluzioni di livello 2 scalabili (in grado di gestire l'aumento del carico). Spesso vengono implementate soluzioni fuori catena (o di terze parti) per risolvere eventuali problemi nel primo livello del protocollo. Queste soluzioni non ostacolano le caratteristiche del primo livello, ma piuttosto le aggiungono.
* Layer 3, anche noto come application layer. Il compito principale di questo livello è quello di ospitare le DApp e molti altri protocolli che abilitano altre applicazioni. In questo caso, il protocollo della blockchain è suddiviso in due livelli secondari significativi, vale a dire l'applicazione e l'esecuzione. Si tratta della soluzione più potente per separare le blockchain con funzionalità cross-chain per raggiungere l'obiettivo di una reale interoperabilità.

###### Scalabilità sul layer 1

Le soluzioni blockchain di livello 1 contribuiscono a migliorare i protocolli di base (ad esempio il proof-of-work o PoW di Bitcoin) modificando il loro funzionamento per quanto riguarda l'elaborazione dei dati. Ad esempio, la rete Ethereum sta passando a un algoritmo di consenso proof-of-stake (PoS), definita come *Ethereum 2.0*.

* Ethereum è forse la migliore rete blockchain di livello 1 da utilizzare come caso di studio. È passata da proof-of-work a proof-of-stake. Nel primo caso poteva elaborare solo circa 10 transazioni al secondo. Ma la seconda ha aumentato il carico di elaborazione dei dati di Ethereum a circa 32 blocchi. Sebbene Ethereum abbia ancora molta strada da fare in termini di scalabilità, il passaggio a PoS è un passo monumentale in questa direzione.

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. Alcuni cambiamenti sono fatti per i canbiamenti sulla chain principale, con due soluzioni principali: Segwit e Sharding.

* 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.

Altra soluzione citata è lo sharding, dividendo come detto la rete blockchain in vari segmenti, ciascuno governato da un gruppo specifico di nodi. In questo modo, le performance saranno aumentata e si ridurrà il tempo di risposta.

* Nello sharding, una rete blockchain è divisa in diversi segmenti, chiamati shard, e ogni shard è governato da determinati nodi che gli sono stati assegnati. Ciò consente alla rete di elaborare più transazioni contemporaneamente, aumentando il throughput complessivo e la capacità della rete.

* Questo approccio può essere utile in situazioni in cui il numero di transazioni sulla blockchain è elevato e la rete fatica a tenere il passo con la domanda. Lo sharding può anche contribuire ad aumentare la scalabilità della blockchain di una rete, in quanto è possibile aggiungere più nodi a uno shard man mano che la rete cresce. Tuttavia, lo sharding comporta anche una serie di sfide, tra cui il mantenimento della sicurezza e dell'integrità della rete e la garanzia di una comunicazione efficiente e sicura tra i diversi shard.

###### Scalabilità sul layer 2

Le soluzioni off-chain, note anche come soluzioni di scalabilità della blockchain di secondo livello, sono metodi utilizzati per aumentare l'efficienza e la velocità delle transazioni su una rete blockchain. Queste soluzioni aggiungono un livello secondario alla rete blockchain principale, progettato specificamente per gestire un volume elevato di transazioni.

Le transazioni vengono scaricate dalla blockchain principale al livello secondario per risparmiare spazio e ridurre la congestione della rete, con tempi di conferma più rapidi e una rete più efficiente. Le soluzioni off-chain offrono anche ulteriori vantaggi in termini di sicurezza e privacy, poiché il livello secondario gestisce la maggior parte delle transazioni, lasciando la blockchain principale per le transazioni più importanti o complesse; le transazioni sul livello secondario potrebbero non essere visibili all'intera rete.

Possiamo citare varie soluzioni:

* i canali, che permettono di creare un canale peer-to-peer tra due parti. Le parti possono scambiare una quantità illimitata di transazioni fuori dalla catena (sul livello 2), mentre inviano solo due transazioni al livello 1 della mainchain, che sono:
  + (i) Una è la prima transazione che apre la connessione tra il livello 1 della mainchain e il livello 2 del canale.
  + (ii) Un'altra transazione memorizzata sul livello 1 è la transazione che chiude la connessione tra il livello 1 e il livello 2.
* Togliendo la maggior parte delle transazioni dal livello 1 (transazioni fuori catena), i canali di livello 2 migliorano la velocità delle transazioni e riducono la congestione della rete, le commissioni e i ritardi delle transazioni.
* I tipi di canali più diffusi sono i canali di stato e i canali di pagamento. I canali di pagamento si occupano dei pagamenti, mentre i canali di stato si occupano degli aggiornamenti di stato generali.
  + i canali di stato (state channels), che facilitano la comunicazione bidirezionale tra una blockchain e i canali transazionali off-chain e migliorano la capacità e la velocità complessiva delle transazioni. Un canale di stato non richiede la convalida da parte dei nodi della rete Layer-1. I canali di stato si occupano dell'aggiornamento dello stato su una rete Blockchain.
    - Si tratta invece di una risorsa adiacente alla rete che viene sigillata utilizzando un meccanismo di firma multipla o di smart contract. Quando una transazione o un lotto di transazioni viene completato su un canale di stato, lo "stato" finale del "canale" e tutte le sue transizioni inerenti vengono registrate sulla blockchain sottostante.
    - Di fatto, si possono scambiare molte transazioni off-chain, inviando solo due transazioni sul layer base. I partecipanti devono essere noti da subito e devono bloccare i propri fondi in un contratto a firma multipla (multi-sig); inoltre, questa soluzione è specifica ad un’applicazione e non può essere considerabile general purpose.
  + Vediamo di capire i canali di stato attraverso un esempio. Supponiamo che due giocatori vogliano giocare a tris su Ethereum Blockchain. A tal fine,
  + (i) Per prima cosa, i giocatori creano uno smart contract multi-firma sulla mainchain di Ethereum che contiene le regole del tic-tac-toe, le informazioni sui giocatori e il premio in denaro 1ETH per il vincitore.
  + (ii) Poi i giocatori entrano nel canale di stato e iniziano a giocare. Ogni mossa del giocatore crea una transazione fuori dalla catena che viene memorizzata nello smart contract.
  + (iii) Quando c'è un vincitore, i giocatori chiudono il canale firmando lo stato finale e sottoponendolo al contratto multi-firma. Lo stato finale del contratto viene quindi memorizzato sulla mainchain di Ethereum e il premio in denaro 1ETH viene trasferito al vincitore.
  + i payment channels, che sono simili ai canali di stato, ma si occupano solo di pagamenti. Ad esempio, il canale di pagamento utilizzato dalla Blockchain Bitcoin è la rete Lighting, mentre il canale di pagamento utilizzato dalla Blockchain Ethereum è Raiden. I canali consentono di creare canali di pagamento peer-to-peer tra due parti. Le due parti possono trasferire fondi tra di loro all'infinito, senza il coinvolgimento del livello 1. Alla fine, quando le due parti decidono di terminare la transazione, possono chiudere il canale. Lo stato finale della transazione viene quindi registrato sul livello 1 della Blockchain.
  + Tutte le transazioni che avvengono all'interno del canale sono fuori dalla catena e non è richiesto il consenso globale. Di conseguenza, queste transazioni vengono eseguite rapidamente tramite uno smart contract, con commissioni molto più basse e alla velocità della luce.
    - Un tipico canale di pagamento prevede tre fasi:
      * Fase uno: stabilire un canale firmando e finanziando un canale
      * Fase due: transazioni peer to peer su un canale di pagamento
      * Fase tre: chiusura del canale e trasmissione dello stato finale alla blockchain principale
    - (i) Per aprire un canale di pagamento, i due partecipanti devono prima depositare alcune monete nel portafoglio a firma multipla (maggiori dell'importo totale coinvolto nelle transazioni successive). È la prima transazione che apre il canale e viene registrata sul livello 1 di Bitcoin.
    - (ii) Dopo che il denaro è stato depositato, entrambi i partecipanti possono effettuare un numero illimitato di transazioni senza interagire con il livello 1. Questo può avvenire un numero illimitato di volte fino a quando non viene registrato nel livello 1. Ciò può avvenire un numero illimitato di volte, purché il saldo del portafoglio sia sufficiente.
    - (iii) Se uno dei partecipanti bara, tutti i fondi presenti nel canale saranno inviati a un altro partecipante come penalità.
    - (iv) Quando i partecipanti hanno terminato le transazioni, firmano lo stato finale della transazione con le loro chiavi private e il canale viene chiuso. Lo stato finale della transazione viene quindi registrato e il saldo viene trasferito ai partecipanti sulla mainchain.
  + Il risultato finale di questo sistema è che Bob e Alice devono pagare solo due transazioni sulla catena per aprire e chiudere il canale di pagamento. Mentre il canale di pagamento è aperto, milioni di trasferimenti possono essere effettuati a costo zero e a velocità inferiori al secondo, direttamente peer to peer: un classico esempio di scalabilità.
* Vantaggi dei canali:
  + (i) sottraendo le transazioni al livello 1 (transazioni fuori catena), il livello 2 decongestiona la rete del livello 1 e di conseguenza aumenta la velocità delle transazioni. Ad esempio, la Blockchain principale di Bitcoin (livello 1) può gestire circa 10 transazioni al secondo, ma la Lightning Network (livello 2) può gestire da migliaia a milioni di transazioni al secondo.
  + (ii) Grazie alla diminuzione delle commissioni di transazione, i micropagamenti sono fattibili. Ad esempio, i canali di pagamento possono consentire agli utenti di pagare anche beni e servizi di piccole dimensioni, come il caffè, senza influenzare la rete Blockchain principale.
* Limitazioni:
  + (i) Per le transazioni, i partecipanti devono rimanere sempre online e utilizzare le loro chiavi private per accedere. Questo li rende vulnerabili a hacking e furti se gli aggressori decifrano le chiavi private.
  + (ii) I partecipanti devono bloccare una certa quantità di fondi in un portafoglio multi-firma per poter aprire il canale di pagamento. Mantenere le monete in un portafoglio caldo su un cellulare, un server o un PC le rende più vulnerabili agli attacchi online, con conseguente furto di monete. D'altro canto, un portafoglio freddo non è collegato a Internet, il che lo rende più sicuro ma meno conveniente.
* le nested blockchain, essenzialmente una blockchain all'interno - o meglio, in cima - a un'altra blockchain. L'architettura della blockchain annidata prevede in genere una blockchain principale che stabilisce i parametri per una rete più ampia, mentre le esecuzioni vengono effettuate su una rete interconnessa di catene secondarie. Su una catena principale possono essere costruiti più livelli di blockchain, con ogni livello che utilizza una connessione genitore-figlio. La catena madre delega il lavoro alle catene figlie che lo elaborano e lo restituiscono alla catena madre una volta completato. La blockchain di base non partecipa alle funzioni di rete delle catene secondarie, a meno che non sia necessaria la risoluzione di controversie.
* i rollup, in cui le transazioni avviate sulla mainchain vengono eseguite sul livello 2. Quindi i dati delle transazioni eseguite vengono raggruppati o arrotolati in un unico blocco e quindi pubblicati sul livello 1 della mainchain. Poi i dati delle transazioni eseguite vengono raggruppati o arrotolati in un unico blocco e quindi inviati al livello 1 della mainchain. La soluzione di scaling ha così preso il nome di "rollup". Di conseguenza, il livello 1 viene alleggerito, poiché tutto il lavoro di calcolo viene svolto fuori dalla catena, sul livello 2. In questo modo è possibile elaborare più transazioni in parallelo, rendendo la rete Blockchain scalabile. Inoltre, come i canali e il plasma, anche i rollup si affidano alla sicurezza della catena principale.
* Come funzionano?
  + (i) C'è un "contratto rollup" sulla mainchain che memorizza la radice di stato del livello rollup. La radice di stato è la radice Merkle dello stato corrente del rollup. L'albero di Merkle è derivato da tutte le transazioni del rollup.
  + (ii) Quando avvengono transazioni sul livello rollup, la radice di stato (Merkle root) cambia. Ciò significa che la radice di stato deve essere aggiornata nel contratto rollup sulla mainchain. A tal fine, le transazioni eseguite vengono compresse, raggruppate e pubblicate sul contratto rollup insieme alla radice di stato aggiornata. Oltre alla radice di stato aggiornata, il batch di transazioni eseguite include i saldi dei conti degli utenti, gli indirizzi, il codice del contratto, ecc. L'intero Merkle tree è memorizzato sul rollup di livello 2, non sulla mainchain.
  + (ii) Il batch di transazioni eseguite è memorizzato sulla mainchain in forma altamente compressa insieme alla radice di stato precedente (radice di Merkle prima dell'elaborazione delle transazioni) e alla radice di stato nuova (radice di Merkle dopo l'elaborazione delle transazioni).
  + (iv) Il contratto di rollup controlla che la radice di stato precedente nel batch corrisponda alla sua radice di stato attuale; se corrisponde, passa la radice di stato alla radice di stato appena aggiornata.
* Vi sono due approcci principali:
  + Optimistic Rollup (OR), come suggerisce il nome all'inizio, presuppongono che i dati delle transazioni inviati alla rete Ethereum siano corretti e validi. Ogni volta che c'è una transazione non valida, c'è una risoluzione della controversia. Essi vengono eseguiti s una VM compatibile con Ethereum, cioè la OVM (Optimistic Virtual Machine), eseguendo gli stessi smart contract eseguiti su Ethereum.
    - Una parte invia un lotto di dati di transazione a Ethereum e, se qualcuno rileva una transazione fraudolenta, può offrire una prova di frode contro quella transazione. In questo caso entrambe le parti, quella che invia il lotto di dati della transazione e quella che presenta la prova di frode, hanno i loro ETH puntati.
    - Ciò significa che qualsiasi comportamento scorretto da parte di una delle due parti comporterà la perdita dei loro ETH. Ogni volta che viene presentata una prova di frode, la transazione sospetta viene eseguita nuovamente, questa volta sulla rete principale di Ethereum.
    - Per assicurarsi che la transazione venga riprodotta con l'esatto stato in cui è stata originariamente eseguita sulla catena rollup, viene creato un contratto manager che sostituisce alcune chiamate di funzione con uno stato della catena rollup.
    - Alcuni esempi: Optimism, Arbitrum
  + Gli OR pubblicano solo il minimo indispensabile di informazioni sulla mainchain, generando prove solo in caso di frode - una dinamica che li rende "ottimisti". Per questo motivo, gli zk-Rollup sono talvolta definiti "prove di validità", mentre gli OR sono noti come "prove di frode". Praticamente chiunque può diventare un aggregatore bloccando un'obbligazione nello smart contract OR. Ecco come funziona l'intero processo:
    - Quando gli utenti inviano transazioni a Optimistic Rollup fuori dalla catena, gli aggregatori si iscrivono e le prove di frode vengono commesse.
    - L'aggregatore distribuisce la transazione localmente per generare un nuovo smart contract. Dopo aver calcolato la nuova radice di stato (radice di Merkle), l'aggregatore invia la transazione e la radice di stato alla catena principale.
    - Se gli utenti ritengono che un aggregatore abbia restituito una radice di stato fraudolenta, compresa una transazione non valida, possono sfidare l'aggregatore.
    - Gli utenti possono lanciare la sfida pubblicando la radice di stato corretta e le prove Merkle necessarie per convalidarla.
    - L'aggregatore che ha commesso l'infrazione, e tutti quelli che hanno costruito sopra il blocco non valido, vedranno la loro obbligazione tagliata, e il ricavato andrà all'utente che ha fatto la segnalazione.
  + Una volta identificato un blocco non valido e completata la prova di frode, la catena Layer-2 torna indietro, riprendendo dal blocco precedente non fraudolento. Mentre alcuni ritengono che gli OR permettano una maggiore supervisione, altri sottolineano le seguenti sfide:
    - Stato non valido: Gli OR consentono l'esistenza di uno stato non valido della blockchain. Di conseguenza, uno stato non valido può esistere finché non viene presentata una prova di frode, il che potrebbe non verificarsi mai.
    - Sicurezza: A causa del loro modello basato sulla teoria dei giochi, gli OR possono essere più vulnerabili agli attacchi. Poiché gli utenti possono impegnarsi nella segnalazione di frodi, ci sono più opportunità di esiti negativi.
    - Scalabilità: In alcuni casi, gli OR possono richiedere più risorse computazionali della catena principale man mano che le transazioni aumentano, con conseguenti costi più elevati.
  + Nonostante queste sfide, molte aziende continuano a esplorare lo sviluppo di Optimistic Rollups e la tecnologia sta rapidamente migliorando. Qui di seguito, discutiamo alcuni dei progetti OR più importanti.
    - Optimism Ethereum (OE)
      * Come altre soluzioni di rollup, Optimism Ethereum (OE) funziona come un protocollo di scalatura Layer-2 per le applicazioni Ethereum. In breve, la piattaforma emula l'esperienza degli sviluppatori della Ethereum Virtual Machine (EVM), facilitando la creazione e la distribuzione di soluzioni rollup compatibili. Inoltre, secondo la documentazione di OE, il protocollo supporta gli smart contract Solidity esistenti, le integrazioni di portafogli off-chain e le interfacce utente (UI).
    - Arbitrum
      * Come gli altri rollup, la catena Arbitrum Rollup esiste in cima alla blockchain di Ethereum come soluzione di livello 2. Inoltre, Arbitrum consente una catena di rollup di tipo "off-chain". Inoltre, Arbitrum consente un'esperienza familiare per sviluppatori e utenti supportando le seguenti funzionalità:
        + Interfaccia Ethereum Remote Procedure Call (RPC): Il protocollo utilizza il protocollo di comunicazione Ethereum, garantendo la compatibilità con le integrazioni di terze parti.
        + Supporto completo per EVM: Arbitrum ha un supporto completo per l'EVM, il che significa che tutti i linguaggi di smart contract sono compatibili con la mainchain di Ethereum.
        + Strumenti Ethereum: Allo stesso modo, il protocollo utilizza strumenti Ethereum di frontend come Truffle, Hardhat, The Graph ed ether.js, integrando ulteriormente Arbitrum con Ethereum.
  + Rete Boba
    - Boba Network è un Optimistic Rollup che fonde strumenti OE open-source con la ricerca e lo sviluppo di OMG Foundation ed Enya. La piattaforma risultante utilizza la tecnologia di Enya che preserva la privacy e l'alto rendimento e le basse tariffe di OMG Plasma. Boba si basa su Secure Multi-Party Computation (SMPC), che consente l'analisi collaborativa dei dati senza rivelare dati sensibili e permette di condurre calcoli congiunti che mantengono la sicurezza dei dati mantenendo il controllo su chi riceve i risultati verificati.
    - Questa struttura è progettata per supportare dApp veloci, a basso costo e private. Il team di Boba ha scelto di basarsi su OE perché il protocollo è quasi identico alla mainchain di Ethereum. Di conseguenza, la compatibilità con EVM e Solidity persiste, semplificando la migrazione degli smart contract da Ethereum (Layer 1) a Boba (Layer 2).
    - Per introdurre la governance DAO nella rete Boba, la OMG Foundation sta lanciando un token di governance Boba (BOBA). Nell'ambito di questa iniziativa, i titolari di OMG esistenti riceveranno BOBA in rapporto 1:1 tramite un airdrop, distribuendo il token a un maggior numero di partecipanti ed espandendo l'ecosistema Boba.
  + Una delle principali limitazioni degli Optimistic rollups è il tempo di prelievo più lungo. Se qualcuno sospetta che una transazione sia fraudolenta, può contestarla e presentare la prova di frode entro 7 giorni. Pertanto, gli utenti devono attendere circa una settimana per ritirare i propri beni dai rollup di livello 2.
* le sidechains, semplicemente delle blockchain separate collegate alla blockchain principale. Gli asset sulla mainchain e sulle sidechain (ref) possono essere scambiati a tassi predeterminati utilizzando un peg bidirezionale (2-way peg), banalmente definito come trasferimento tra la catena principale e quella secondaria. Ciò consente di scaricare alcune transazioni e applicazioni dalla mainchain alla sidechain per ridurre la congestione della rete e aumentare la scalabilità della blockchain. Esse sono Ethereum-compatibili (usando sempre la EVM( ed indipendenti dalla catena principale.
  + A differenza di altre soluzioni di livello 2 (canali, plasma e roll-up), che sfruttano la sicurezza del livello 1, le sidechain sono responsabili della propria sicurezza. Un altro punto importante delle sidechain è che hanno bisogno di nodi propri per convalidare le transazioni e creare un blocco. Hanno anche i loro meccanismi di consenso (come POW, POS, Proof of Authority, DPoS, ecc.) e i loro parametri di blocco. I nodi che convalidano i blocchi guadagnano le ricompense per il loro lavoro in una sidechain nello stesso modo in cui funzionano tutte le altre blockchain. Sebbene le sidechain rimangano indipendenti l'una dall'altra, insieme formano un intero ecosistema.
  + Più sidechain possono essere collegate alla mainchain e ogni sidechain può avere la propria architettura. È possibile creare una rete di sidechain con una mainchain in cui la mainchain può agire come una rete di relay e le sidechain rappresentano una rete di blockchain. *Plasma (ethereum)* e *Parachain (polkadot)* sono soluzioni di scala popolari che utilizzano sidechain e relay.
  + Uno sviluppatore potrebbe adottare una sidechain rispetto a un canale di pagamento o di stato se ha bisogno di maggiore flessibilità e controllo sull'infrastruttura sottostante.

Potrebbe trattarsi del lancio di un token o di una DApp, pur sfruttando i bassi costi e la maggiore velocità consentiti dal fatto di non implementare gli smart contract direttamente sulla L1.

* Il compito principale delle sidechain è:
  + elaborare e convalidare i dati per la catena principale
  + o aggiungere funzionalità, come l'esecuzione di contratti intelligenti per le blockchain che non sono in grado di farlo, come Bitcoin.
  + le sidechain comunicano con la mainchain tramite un peg bidirezionale (2WP); di conseguenza, le sidechain sono chiamate anche pegged sidechain.
* *Two-way peg (2WP)*: Il 2WP funge da intermediario per facilitare il trasferimento di beni o monete dalla mainchain (livello 1) alla sidechain (livello 2) e viceversa. Sotto il cofano, le monete non vengono trasferite, ma vengono temporaneamente bloccate sulla mainchain creando una transazione. Una seconda transazione viene generata per sbloccare la stessa quantità di monete equivalenti in una sidechain.
  + Le monete sulla mainchain possono essere sbloccate solo quando la quantità equivalente di monete sulla sidechain viene nuovamente bloccata. Questo per evitare la presenza di monete libere su entrambe le catene e prevenire il problema della doppia spesa. Il sistema 2WP consente alle parti interessate di entrare in una transazione sulla sidechain senza rivelare le informazioni all'intera rete.
* *Presenza della terza parte*: La terza parte/autorità è responsabile delle funzioni di blocco e rilascio tra le sidechain e le mainchain. Viene avviata una transazione per bloccare le monete. Dopo aver raggiunto il consenso tra i nodi, il blocco firmato viene inviato alla mainchain. Questo blocca automaticamente le monete sulla mainchain.
  + L'autorità fidata che controlla il peg a due vie emette quindi una somma equivalente di monete nella sidechain alle parti della transazione. Le parti possono quindi effettuare una serie di transazioni all'interno dei confini della sidechain. Una volta effettuate le transazioni, l'autorità verifica le transazioni e rilascia le monete corrispondenti nella mainchain sbloccandole.
  + L'intera struttura della sidechain si basa sul peg a due vie e sull'autorità fidata per mantenere l'integrità delle transazioni tra le due catene. La presenza di un'autorità può portare alla centralizzazione della rete dandole troppo potere.
* *Prove SPV*: La prova SPV (Simple Payment Verification) è un modo per dimostrare crittograficamente che le monete sono bloccate sulla mainchain per essere utilizzate sulla sidechain. Invece di controllare tutte le transazioni precedenti, cosa che sarebbe lenta, una SPV prova anche se la transazione avviata sulla mainchain è valida e fa parte del blocco valido. Grazie agli SPV, i nodi della sidechain non devono scaricare l'intera Blockchain principale ogni volta che è necessario il processo di verifica. Le blockchain di Bitcoin ed Ethereum supportano le SPV sotto forma di Merkle proof. Le prove Merkle includono la radice Merkle e il percorso Merkle.
  + Ogni coppia di transazioni sottoposte a hash viene sottoposta a hash insieme dalla funzione di hash e così via finché non si ottiene un hash per l'intero blocco, che viene chiamato Merkle Root o Root hash. D'altra parte, il percorso Merkle è l'insieme dei valori hash necessari per generare l'hash radice.
  + I nodi della catena laterale ripetono l'operazione di hash per calcolare il valore hash radice. Se il valore di root hash ottenuto dal processo corrisponde al valore di root hash presente nell'SPV, significa che è stata avviata una transazione che ha bloccato le monete sulla mainchain.
* Vantaggi:
  + (i) Le sidechain aumentano il throughput delle transazioni, eliminando la maggior parte delle transazioni nella loro sidechain ed elaborando le transazioni a una velocità molto più elevata. Inoltre, riducono in modo significativo le commissioni di transazione. Ad esempio, Polygon, una sidechain di Ethereum, sostiene di aver raggiunto una scalabilità di 65000 transazioni al secondo, con commissioni di transazione di circa 1 dollaro.
  + (ii) Le blockchain pubbliche sono trasparenti e aperte alla verifica. Ogni transazione è registrata e può essere verificata da qualsiasi partecipante. Tuttavia, per le imprese, le blockchain pubbliche non sono utili a causa del rischio di rivelare molte informazioni specifiche dell'azienda. Con le sidechain, invece, è possibile mantenere la privacy delle transazioni. I dati relativi alle transazioni aziendali risiedono nella sidechain, mentre la mainchain funge da archivio per la verifica dei dati con hash. Mentre la mainchain è pubblica e senza permessi, la sidechain è progettata in modo privato e con permessi per soddisfare le esigenze aziendali. I dati specifici dell'azienda possono essere archiviati in modo sicuro nella sidechain e quindi molto più sicuri e immuni da hacking.
* Sfide:
  + La maggior parte delle sidechain sono un po' più centralizzate rispetto alla mainchain, per cui offrono un compromesso tra sicurezza e velocità. Pertanto, le informazioni che vengono esternalizzate sulla sidechain possono essere selezionate, mentre i dettagli più sensibili rimangono sulla mainchain per mantenere la sicurezza.

## Soluzioni di scalabilità

#### Layer 1

##### Algorand

Algorand è un protocollo blockchain di livello 1 che utilizza un consenso PPoS (Pure Proof of Stake) modificato. Il meccanismo PPoS consente a ogni titolare di ALGO, anche con un solo token ALGO, di guadagnare ricompense quando il protocollo blockchain viene utilizzato da altre persone. Questa disposizione abbassa la barriera d'ingresso per le scommesse su Algorand. Tuttavia, una barriera d'ingresso così bassa può rendere la rete vulnerabile agli attori malintenzionati.

* Esso utilizza un'architettura a due livelli per essere più scalabile. Il primo livello è riservato alle transazioni più complesse legate ai protocolli Defi, mentre il secondo livello o catena gestisce transazioni semplici come il trasferimento di token. Questo meccanismo a due livelli consente ad Algorand di raggiungere un TPS fino a 1.000, superando il TPS di Ethereum di 14'17 transazioni. Algorand ospita attualmente oltre 100 DApp, rispetto alle 3.000 di Ethereum. Se Algorand raggiungerà la scala di attività gestita da Ethereum, sarà in grado di mantenere il suo elevato TPS è ancora da vedere.

Grazie a una serie di miglioramenti, tra cui l'esclusivo approccio "pure-proof-of-stake" (PPoS) (il protocollo proof-of-stake di Algorand) utilizzato per raggiungere il consenso decentralizzato, la blockchain di Algorand supera i precedenti protocolli blockchain. Il PPoS è stato progettato per evitare il problema dei "ricchi che diventano sempre più ricchi". In sostanza, mentre PoS paga i minatori con la puntata più alta, PPoS seleziona i minatori a caso, indipendentemente dal loro investimento nel sistema.

* Protocollo di accordo bizantino (Byzantine agreement protocol)

Quando il PPoS è abbinato a un protocollo di accordo bizantino (BA), il meccanismo determina le modalità di adesione alla rete decentralizzata, disincentiva le attività fraudolente e produce un'unica fonte di verità che può essere verificata.

Il meccanismo di accordo bizantino è scalabile per molti utenti e consente ad Algorand di raggiungere il consenso su un nuovo blocco con una bassa latenza e senza biforcazioni. L'uso di funzioni casuali verificabili (VRF) per scegliere casualmente gli utenti in modo privato e non interattivo è un metodo fondamentale che rende BA adatto ad Algorand. La VRF è una funzione pseudorandom a chiave pubblica che genera la prova che i suoi risultati sono accurati.

Il blocco concordato viene quindi confermato e trasmesso attraverso la rete utilizzando varie firme digitali dei verificatori appropriati. Poiché solo un blocco può avere la soglia richiesta di voti del comitato su Algorand, due blocchi non possono mai essere aggiunti alla catena nello stesso momento. Ciò significa che in una rete adeguatamente decentralizzata, tutte le transazioni vengono completate in pochi secondi, garantendo la velocità.

* Architettura blockchain a due livelli

Algorand utilizza un design della blockchain a due livelli per mantenere la velocità durante l'esecuzione di applicazioni complesse. Il livello 1 consente di creare Algorand Standard Assets (ASA). Gli ASA rappresentano token nuovi o esistenti sulla blockchain, swap atomici e semplici smart contract Algorand.

Il livello 2 è destinato a contratti intelligenti più complicati e ad applicazioni decentralizzate che vengono eseguite fuori dalla catena. Questo metodo consente alla blockchain di Algorand di gestire le transazioni a una velocità paragonabile a quella delle grandi reti di pagamento.

* Posizionamento per la sicurezza (Staking for security)

Chiunque desideri contribuire alla sicurezza della rete Algorand può utilizzare un conto che possiede ALGO, la criptovaluta di Algorand, cioè il token nativo della blockchain, per dichiarare il proprio interesse. La possibilità di essere scelti è determinata dalla quantità di ALGO che un utente possiede rispetto agli altri utenti della rete che hanno espresso interesse a partecipare.

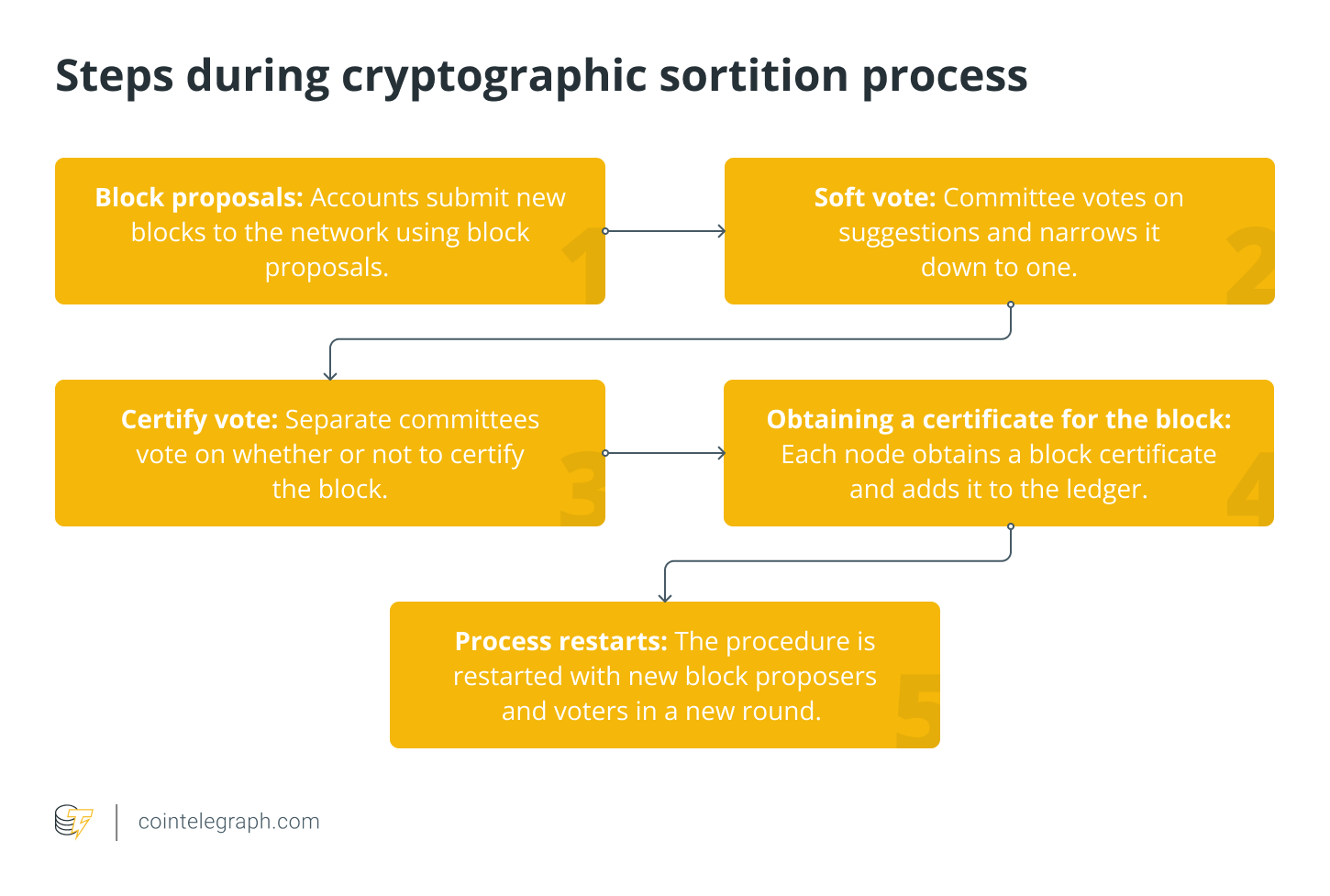
Tuttavia, Algorand incontra tre ostacoli. In primo luogo, Algorand deve proteggersi dai sybil attack, in cui un attaccante genera un gran numero di pseudonimi per influenzare il protocollo di accordo bizantino.

In secondo luogo, BA deve incorporare milioni di utenti, scalando in modo significativo rispetto a quanto possono gestire gli attuali protocolli di accordo bizantino. Infine, Algorand deve essere resistente agli attacchi denial-of-service, consentendo di continuare a funzionare anche se un attaccante disconnette alcuni utenti.

Algorand applica diverse tecniche per risolvere i problemi di cui sopra, come spiegato nelle sezioni seguenti:

* Utenti ponderati
  + Il protocollo è in grado di gestire gli utenti disonesti finché gli utenti onesti che seguono le raccomandazioni del protocollo rappresentano più di due terzi della posta totale del sistema.
* Consenso per comitato
  + BA raggiunge la scalabilità assegnando ogni fase del suo protocollo a un comitato, un piccolo gruppo di rappresentanti scelti a caso dal numero totale di utenti in base ai loro pesi. Di conseguenza, Algorand può garantire che un numero sufficiente di membri del comitato sia sincero.
* Sostituzione dei partecipanti
  + Una volta che un membro del comitato invia un messaggio in BA, un nemico può prendere di mira quel membro. BA contrasta questa minaccia consentendo ai membri del comitato di parlare una sola volta. Di conseguenza, una volta che un membro del comitato rivela il proprio nome a un avversario, non è più importante per il BA.
  + BA raggiunge questa qualità evitando qualsiasi stato privato (a parte la chiave privata dell'utente), consentendo a tutti gli utenti di partecipare allo stesso modo ed eleggendo nuovi membri del comitato per ogni fase del protocollo di accordo bizantino.
* Selezione crittografica
  + BA sceglie i membri del comitato in modo riservato e non interattivo per evitare che un nemico li prenda di mira. Ciò significa che ogni utente del sistema può decidere autonomamente se vuole far parte del comitato.
  + Se l'utente viene scelto, la funzione produce una breve stringa che dimostra agli altri utenti la sua appartenenza al comitato e che l'utente può includere nei suoi messaggi di rete. Ad esempio, un avversario non sa quale utente prendere di mira finché non inizia a partecipare al BA, poiché la selezione dei membri non è interattiva.

I passi seguiti sono i seguenti:



Riferimento: <https://cointelegraph.com/learn/what-is-algorand>

* Come funziona Algorand?
  + Nella rete Algorand ci sono due tipi di nodi: i nodi di partecipazione e i nodi relay. I nodi relay fungono da hub della rete, mantenendo il collegamento tra Algorand e il resto dei nodi del sistema. I nodi di partecipazione forniscono potenza di calcolo per convalidare le transazioni e sono quelli che ottengono le ricompense più significative.
  + I nodi relay sono utilizzati dai nodi di partecipazione per connettersi e tenere traccia del libro mastro. Chiunque può gestire un relay o un nodo di partecipazione in Algorand, ma mentre i nodi di partecipazione sono pagati per i loro sforzi, i nodi relay non possono "minare" ALGO. La Fondazione Algorand ha invece stabilito un sistema di ricompense per i nodi relay che scadrà tra due e cinque anni. Per connettersi alla rete Algorand, hanno bisogno di un software di virtualizzazione chiamato Algorand Virtual Machine (AVM).
  + L'AVM è un software che opera sia sui nodi relay che su quelli di partecipazione alla rete Algorand. Lo stack engine della AVM è responsabile della valutazione degli smart contract sulla rete Algorand. Inoltre, l'AVM valuta tutta la logica contenuta negli smart contract prima di decidere se eseguirli o meno.
  + Gli smart contract sono gestiti da Algorand in due livelli: on-chain e off-chain. Nel livello 1, il sistema consente agli smart contract di funzionare "on-chain", come la blockchain di Ethereum. Ciò significa che ogni contratto smart aggiunge traffico alla rete e che un numero eccessivo di contratti smart può causare un rallentamento della rete.
  + Per ovviare a questo problema, Algorand offre anche smart contract di livello 2, che vengono eseguiti "fuori catena". Il contratto intelligente non aggiunge traffico alla rete, ma viene eseguito al di fuori della rete e registrato nel libro mastro della blockchain.

#### Layer 2

##### Plasma

Plasma è un'altra soluzione di scalabilità di livello 2. Plasma sfrutta i contratti intelligenti e gli alberi di Merkle per creare un numero illimitato di catene figlio copie della Blockchain principale (Ethereum Blockchain). Lo scarico delle transazioni dalla catena principale (livello 1) alle catene figlie (livello 2) consente transazioni veloci ed economiche. Come le sidechain, ogni catena figlia è trattata come una blockchain separata con il proprio meccanismo di consenso, i propri nodi, le proprie dimensioni e il proprio tempo di blocco.

* Come i canali, il plasma sfrutta la sicurezza della mainchain. La mainchain e le catene figlio sono legate tra loro attraverso "contratti intelligenti" che contengono le regole che guidano ogni catena figlio. I contratti fungono da ponte che consente ai partecipanti di spostare beni digitali/monete tra la mainchain e le catene figlio. Inizialmente, tutte le transazioni devono essere create sulla catena principale.
* Se vengono rilevati sospetti o frodi nelle catene figlio del plasma, gli utenti del plasma possono uscire dalla catena del plasma e passare alla catena principale.
* Come funziona Plasma?
  + L'operatore della catena figlio stabilisce le regole di funzionamento della catena figlio.
  + Le transazioni elaborate rimangono nelle catene plasma. Ma le intestazioni dei blocchi (contenenti le radici di Merkle) di ogni blocco delle catene plasma vengono inviate e registrate nei blocchi della mainchain. Ciò riduce la congestione della rete della mainchain, consentendo così l'elaborazione simultanea di decine di migliaia di transazioni nelle catene del plasma.
  + I dati delle catene minori vengono convalidati utilizzando le "prove di frode". Le prove di frode sono un meccanismo che consente a chiunque di determinare se i dati non sono validi utilizzando le prove di Merkle. Ad esempio, quando si verifica una frode in una catena di plasma, sia che si tratti di un caso di doppia spesa o di un incasso superiore a quello di tutti i conti, chiunque può fornire una prova di frode per dimostrare che la transazione non è valida. Se la frode è provata, la transazione viene annullata.
* Vantaggi:
  + Le catene Plasma sono più vantaggiose dei canali perché si possono inviare asset/monete a chiunque, mentre con i canali la transazione può avvenire solo tra due parti.
  + Il vantaggio delle catene Plasma rispetto alle sidechain è che la catena Plasma è protetta dalla catena principale. Se la sidechain viene attaccata, non succede nulla alla mainchain, ma la mainchain non può fare nulla per proteggere gli utenti della sidechain. Mentre, poiché le catene di plasma sfruttano la sicurezza della mainchain, in caso di attacco gli utenti della catena di plasma possono uscire e passare alla mainchain. Pertanto, la sicurezza di plasma è maggiore rispetto alle sidechain.
* Limitazioni:
  + Uno degli svantaggi di plasma è un lungo periodo di attesa per gli utenti che vogliono ritirare le loro monete dal livello 2 e trasferirle al livello 1. (ii) Gli utenti devono aspettare per poter accedere alla catena principale.
  + Gli utenti devono attendere almeno 7-14 giorni per il prelievo. Questo tempo è necessario per verificare che la transazione di prelievo non sia fraudolenta.

Esempi: Il progetto che sfrutta la potenza di Plasma su Ethereum è OMG.

##### Polygon

Polygon è una soluzione di scalabilità di livello 2 per la blockchain Ethereum. Polygon agisce come una blockchain più veloce in esecuzione simultanea con la blockchain Ethereum che utilizza più sidechain.

* Si rivolge alle diverse esigenze degli sviluppatori fornendo strumenti per creare applicazioni decentralizzate scalabili (dApp) che danno priorità a prestazioni, esperienza utente (UX) e sicurezza. Polygon ottiene questo risultato in gran parte grazie all'architettura tecnica di base della sua catena di commit Proof-of-Stake (PoS) e alla sua soluzione di scalabilità L2 More Viable Plasma (MoreVP). La blockchain PoS di Polygon funge da Commit Chain per la mainchain di Ethereum, attirando sulla sua piattaforma oltre 80 dApp Ethereum che effettuano transazioni senza i casi di congestione della rete comuni a Ethereum e ad altre blockchain Proof-of-Work (PoW).
* Polygon funziona principalmente attraverso le Commit chains, che sono reti di transazioni che operano adiacenti a una blockchain principale, in questo caso Ethereum. Le catene di Commit raggruppano lotti di transazioni e le confermano in massa prima di restituire i dati alla catena principale. In teoria, Polygon potrà disporre di migliaia di catene che scalano insieme per aumentare il throughput, con il potenziale di generare un giorno milioni di transazioni al secondo (TPS) se collegate a una catena principale come Ethereum. Attualmente Polygon si avvale solo della connettività delle catene Commit per migliorare i tempi delle transazioni, ma alla fine si avvarrà anche di altri meccanismi di scalatura Layer-2 come i Rollup ottimistici.

Invece di affidarsi al classico algoritmo Proof-of-Work (PoW), che consuma molta energia durante la creazione di nuovi blocchi, Polygon utilizza il consenso Proof-of-Stake (PoS), che comprende un insieme di validatori di nodi per verificare e validare i blocchi di transazioni. La differenza principale è che i validatori devono impegnarsi nel lavoro (calcoli) nelle reti PoW, mentre i titolari di token convalidano e verificano le transazioni in un protocollo PoS.

In particolare, Polygon utilizza un particolare meccanismo di consenso definito POSDAO (Proof of Stake Decentralized Autonomous Organization), che è un meccanismo di consenso sviluppato dal team di Polygon (precedentemente Matic Network) per convalidare le transazioni e aggiungere nuovi blocchi alla blockchain di Polygon. È un ibrido dei concetti di Proof of Stake (PoS) e di Decentralized Autonomous Organization (DAO).

Ad alto livello, il meccanismo di consenso POSDAO funziona come segue:

* Validatori: Il sistema POSDAO è gestito da un insieme di validatori che sono responsabili della convalida delle transazioni e dell'aggiunta di nuovi blocchi alla blockchain di Polygon. I validatori sono selezionati in base alla loro partecipazione alla rete, cioè al numero di token che hanno puntato.
* Puntata: I validatori devono puntare una certa quantità di MATIC, il token nativo di Polygon, per poter partecipare alla rete. Questa puntata serve come garanzia per assicurare che i validatori si comportino onestamente e seguano le regole della rete. I validatori possono guadagnare ricompense per la loro partecipazione alla rete convalidando transazioni e aggiungendo nuovi blocchi alla blockchain.
* Selezione casuale: I validatori sono selezionati in modo casuale per convalidare le transazioni e aggiungere nuovi blocchi alla blockchain. La probabilità di essere selezionati è proporzionale alla quantità di MATIC che hanno puntato. Ciò significa che i validatori con una puntata maggiore hanno una probabilità più alta di essere selezionati.
* Slashing: i validatori possono essere penalizzati o "slashati" se si comportano male, ad esempio spendendo due volte, non convalidando le transazioni o aggiungendo blocchi non validi alla blockchain. Questa sanzione può includere la perdita dei token puntati, il che incentiva i validatori ad agire onestamente e a seguire le regole della rete.
* Governance: Il sistema POSDAO è governato da un'organizzazione autonoma decentralizzata (DAO) gestita dalla comunità. La comunità può votare le proposte per migliorare la rete, come le modifiche ai requisiti di puntata o al processo di selezione dei validatori. Il processo di governance è trasparente e democratico e consente a tutti i partecipanti alla rete di avere voce in capitolo sul futuro della rete.

Nel complesso, il meccanismo di consenso POSDAO consente tempi di elaborazione delle transazioni più rapidi e commissioni più basse rispetto al meccanismo di consenso Proof-of-Work (PoW) nativo di Ethereum, che è computazionalmente costoso e lento. Inoltre, fornisce un metodo più sicuro e democratico per la convalida delle transazioni e l'aggiunta di nuovi blocchi alla blockchain, poiché i validatori sono selezionati in base alla loro partecipazione alla rete e il processo di governance è gestito dalla comunità.

Gli utenti vengono ricompensati con $MATIC, il token nativo dell'ecosistema Polygon. È possibile guadagnare $MATIC attraverso uno dei seguenti approcci:

* Diventare un validatore. È possibile eseguire un commit sula rete e gestire un nodo completo che convalida le transazioni sulla blockchain. Si ottiene una parte di $MATIC e delle commissioni quando si è un validatore. I vostri $MATIC possono essere ridotti se agite in modo malizioso o lento.
* Diventare un delegatore. Un nodo pubblico che riceve $MATIC da altri per aiutare il protocollo a condurre la convalida Proof-of-Stake. Il potere di voto del delegatore dipende dalla dimensione della quota delegata. Diventare un delegatore è più facile che essere un validatore.

Il token Matic (MATIC) è il token nativo di Polygon e ha diversi usi distinti, uno dei quali è quello di alimentare il protocollo attraverso un meccanismo basato sul gas utilizzato per pagare le commissioni di rete maturate dalla potenza di calcolo che la rete esercita per trasferire i dati. Questo meccanismo consente anche agli sviluppatori di software e ai collaboratori dell'ecosistema di creare dApp su Polygon pagando i token MATIC per utilizzare la piattaforma e il suo framework di sviluppo.

* I MATIC possono essere memorizzati nel Matic Wallet, dando immediatamente ai titolari la possibilità di puntare i propri token e di gestire direttamente i propri investimenti. Matic Wallet è stato progettato utilizzando la tecnologia MoreVP di Polygon come soluzione facile da usare per i possessori di token MATIC per gestire in modo sicuro e semplice le proprie finanze in criptovaluta. Il portafoglio è costruito per essere veloce come un fulmine e si integra con WalletConnect per garantire la custodia delle chiavi private dell'utente e per fornire l'accesso ad altre funzionalità di Polygon. Il portafoglio consente inoltre agli utenti di connettersi a varie dApp, di puntare i propri token MATIC e di detenere altri token ERC-20.

Il token MATIC ha tre casi d'uso principali nell'ecosistema Polygon:

* Gas token. Ogni volta che si effettua una transazione su Polygon o si utilizza un'applicazione basata su Polygon, si paga una piccola tassa in $MATIC. Questa tassa incentiva i vari minatori a elaborare e verificare la transazione che si sta cercando di effettuare.
* Governance. Chi possiede i token $MATIC ha alcuni privilegi speciali. I $MATIC possono essere utilizzati per le proposte di miglioramento di Polygon (PIP) e per le votazioni della governance per decidere la direzione di Polygon.
* Sicurezza della rete. Il meccanismo PoS di Polygon utilizza i token MATIC per raggiungere il consenso sulla rete. Come utente, puoi puntare $MATIC e contribuire alla sicurezza della rete, guadagnando al contempo delle ricompense. Questo approccio garantisce che gli utenti non agiscano in modo disonesto, poiché esiste il rischio di perdere i token MATIC puntati.

Polygon utilizza il framework Plasma, una soluzione di scalabilità di livello 2 che consente transazioni fuori catena. Ciò significa che le transazioni non vengono elaborate direttamente sulla blockchain di Ethereum, bensì sulla sidechain di Polygon. Le transazioni completate vengono poi periodicamente aggregate e impegnate nella blockchain di Ethereum.

* Il framework Plasma consente a Polygon di ottenere tempi di elaborazione delle transazioni più rapidi e commissioni più basse. Questo perché la rete sidechain non è limitata dai vincoli computazionali della rete Ethereum. Al contrario, può elaborare un volume molto maggiore di transazioni in un tempo più breve.
* Polygon consente anche l'interoperabilità tra diverse blockchain grazie all'uso dei bridge. I bridge sono contratti intelligenti che consentono il trasferimento di beni e dati tra Polygon e altre blockchain. Ciò significa che gli utenti possono trasferire beni tra diverse blockchain senza doverli convertire in una specifica criptovaluta o utilizzare uno scambio centralizzato.

Listiamo alcuni casi d'uso reali della rete crittografica Polygon.

* Pagamenti: La piattaforma crittografica Polygon è stata progettata per consentire alle dApp di accelerare i pagamenti, permettendo un regolamento quasi istantaneo dei pagamenti attraverso l'integrazione di un'interfaccia di programmazione delle applicazioni (API) e di un kit di sviluppo software (SDK) specializzati. Questo processo consente alle dApp, ai commercianti e agli utenti di accettare o pagare istantaneamente in qualsiasi tipo di criptovaluta, anche se di solito in token ERC-20 o ETH. Questo sistema è in fase di implementazione in tre fasi distinte:
* Pagamenti in Ethereum (ETH) e token ERC-20
* Trasferimenti e pagamenti cross-chain di token multi-asset utilizzando gli atomic swap in collaborazione con i fornitori di liquidità
* Sistema di pagamento basato su Fiat che utilizza fornitori di liquidità fiat.
* Piattaforma di prestito: Polygon sta costruendo un meccanismo per consentire agli esercenti di analizzare il rating di credito degli utenti che si sono iscritti alla piattaforma valutando la loro storia di transazioni. Questa funzionalità è realizzata in collaborazione con Dharma Protocol. Il principale protocollo di prestito Aave ha più di 1 miliardo di dollari di liquidità bloccata sui suoi mercati Polygon con più di 8000 utenti.
* Giochi: La soluzione di scalabilità della sidechain Layer-2 di Polygon è in grado di rendere i giochi basati sulla blockchain più veloci e performanti. I giochi blockchain sono in ritardo rispetto ai tradizionali sistemi di gioco per PC e console a causa della scarsa velocità delle transazioni e dell'elevata latenza di rete. Con la tecnologia di scalatura Commit Chain di Polygon e la rete Ethereum che lavorano insieme, gli sviluppatori e i giocatori saranno in grado di costruire e giocare in modo più efficace.
  + La capacità di Polygon di contribuire alla crescita dell'industria dei giochi blockchain non potrebbe arrivare in un momento migliore, dato che i token non fungibili (NFT) e i mercati NFT stanno guidando la popolarità dell'industria blockchain e delle criptovalute in generale, con molti giocatori che comprano, vendono e scambiano diversi tipi di NFT nel gioco. Le principali Dapp di gioco e NFT come Aavegotchi, Neon District, Zed Run e Cometh hanno scalato le loro esperienze utente con Polygon.
* Altri casi d'uso: Polygon è stato costruito anche per molti altri casi d'uso, come ad esempio per aiutare a realizzare i tempi di regolamento rapidi necessari per consentire alle borse decentralizzate (DEX) di offrire agli utenti un trading più veloce e più economico. Quickswap, Dfyn e ComethSwap sono alcuni dei DEX Polygon che stanno registrando alti volumi e attività da parte degli utenti. Protocolli come Curve e mStable hanno inoltre garantito scambi di stablecoin a basso costo e a basso slippage. Inoltre, la soluzione di plasma scaling di Polygon è in grado di accelerare gli swap atomici cross-chain di asset tokenizzati e non. La maggior parte delle dApp ha bisogno di un modo per firmare le transazioni senza inviare chiavi private a causa delle preoccupazioni sulla privacy degli utenti. Grazie ai suoi miglioramenti di scalabilità, Polygon contribuisce a creare un quadro di identità aperto per la progettazione e l'utilizzo delle dApp.

##### Lightning Network

La Lightning Network è una soluzione di scala di livello 2 per Bitcoin che mira ad aumentare la velocità delle transazioni e a ridurre le commissioni consentendo agli utenti di effettuare transazioni fuori catena. È stata proposta per la prima volta nel 2015 da Joseph Poon e Thaddeus Dryja ed è ora una soluzione popolare per scalare il Bitcoin.

La Lightning Network funziona creando una rete di canali di pagamento tra due parti. Questi canali di pagamento consentono agli utenti di effettuare transazioni fuori dalla catena, senza la necessità di registrare ogni transazione sulla blockchain di Bitcoin. Invece, la transazione finale viene trasmessa alla rete Bitcoin quando il canale di pagamento viene chiuso.

* Per creare un canale di pagamento, due parti devono prima creare un indirizzo multi-firma sulla blockchain Bitcoin. Questo indirizzo richiede che entrambe le parti firmino ogni transazione che spende i fondi presenti nell'indirizzo. Ciascuna delle parti finanzia poi l'indirizzo con l'importo che desidera transare.
* Una volta creato il canale, le due parti possono effettuare transazioni tra loro senza dover trasmettere ogni transazione alla blockchain Bitcoin. Possono invece aggiornare il saldo del canale di pagamento firmando transazioni che trasferiscono fondi tra i loro conti.

Le due parti possono trasferire fondi l'una all'altra indefinitamente senza informare la blockchain principale. Poiché tutte le transazioni del protocollo di livello 2 non devono essere approvate da tutti i nodi, le transazioni vengono notevolmente velocizzate. I nodi della Lightning Network in grado di instradare le transazioni sono formati dalla combinazione dei singoli canali di pagamento tra le parti interessate. Pertanto, la Lightning Network è il risultato di molti canali di pagamento collegati tra loro.

* Alla fine, quando le due parti decidono di terminare le transazioni, possono chiudere il canale. Tutte le transazioni del canale vengono quindi consolidate in un'unica transazione, che viene inviata alla mainnet Bitcoin per essere registrata. Il consolidamento assicura che molte piccole transazioni non intasino la rete in una sola volta. L'aggregazione in un'unica transazione richiede meno tempo e meno fatica ai nodi per la convalida. Senza canali di pagamento, le transazioni più piccole intralciano quelle più grandi, congestionando la rete e aumentando il carico di lavoro di convalida dei nodi.
* Ad esempio, se Mike si reca ogni giorno in una caffetteria locale e vuole pagare in Bitcoin, può scegliere di effettuare una piccola transazione per ogni tazza di caffè, ma a causa dei problemi di scalabilità di Bitcoin, la transazione può richiedere più di un'ora per essere convalidata. Mike dovrà inoltre pagare le elevate commissioni della rete Bitcoin, anche se sta effettuando una piccola transazione.
* Le piccole transazioni funzionano con i metodi di pagamento tradizionali, come le carte di credito, perché società come Visa hanno l'infrastruttura per elaborare più di 24.000 TPS. Al contrario, Bitcoin, in un giorno normale, può convalidare sette transazioni al secondo.

Con la rete Lightning, Mike può aprire un canale di pagamento con la caffetteria. Ogni acquisto di caffè viene registrato all'interno di quel canale e il negozio viene comunque pagato. La transazione è economica o forse addirittura gratuita, oltre che istantanea. Quando il deposito di Bitcoin di Mike nel canale si esaurisce, può scegliere se chiudere il canale o ricaricarlo. Quando un canale viene chiuso, tutte le sue transazioni vengono registrate nella blockchain principale di Bitcoin.

* La rete Lightning crea un contratto intelligente tra due parti. Le regole dell'accordo sono codificate nel contratto al momento della creazione e non possono essere infrante. Il codice dello smart contract assicura anche che l'adempimento del contratto sia automatico, in quanto i contratti vengono inizialmente creati con requisiti predefiniti che tutte le parti partecipanti accettano.
* Una volta soddisfatti tali requisiti e quando un cliente paga l'importo corretto per un caffè, il contratto viene automaticamente adempiuto senza il coinvolgimento di terzi. Una volta convalidata, la rete Lightning rende anonime le transazioni all'interno di un canale di pagamento. Tutto ciò che si può vedere è il trasferimento totale di valore, non le singole transazioni all'interno di esso.
* È assolutamente possibile condurre transazioni senza alcuna restrizione al di fuori della blockchain. Le transazioni al di fuori della catena possono essere affidabili per far rispettare la blockchain, visto che finiscono sulla mainnet una volta chiusi i canali di pagamento. La mainnet è l'arbitro di tutte le transazioni. Anche se i protocolli off-chain hanno un proprio libro mastro, questo libro mastro si integra sempre nella catena principale, che è il fulcro del progetto di Lightning Network.

La Lightning Network offre i seguenti vantaggi rispetto alla blockchain nativa di Bitcoin.

* Scalabilità
* Velocità
* Supporto per i micropagamenti
* Bassi requisiti energetici

La mancanza di scalabilità è stata una delle caratteristiche più discusse per quanto riguarda la blockchain Bitcoin. L'aggiunta di ogni blocco per ogni transazione ostacolava gravemente la scalabilità della rete. La Lightning Network risolve questo problema togliendo le transazioni dalla blockchain, tenendo conto delle considerazioni sulla sicurezza e sull'anonimato.

Inoltre, poiché le transazioni vengono tolte dalla blockchain principale e portate avanti in blocchi di livello 2, sono molto più veloci ed efficienti. Le transazioni vengono eseguite attraverso un meccanismo di consenso a due parti noto come canale di pagamento. Questo rende la Lightning Network uno dei componenti chiave dell'ecosistema Bitcoin.

La Lightning Network facilita anche i micropagamenti rapidi. Bitcoin impone un output minimo di transazione che è più di 100 volte superiore a quello della Lightning Network. I micropagamenti veloci sono il futuro delle applicazioni Web3 come il gioco d'azzardo e la realizzazione di questo caso d'uso è estremamente importante per l'usabilità della catena.

I micropagamenti veloci sono resi possibili dalla Lightning Network; tuttavia, sono attuabili solo se questi micropagamenti possono essere eseguiti con commissioni di transazione molto basse. La mancanza di un'elaborazione efficiente delle transazioni spesso fa perdere quote di mercato alla blockchain a vantaggio dei suoi concorrenti.

L'ecosistema DeFi su Ethereum ha avuto un notevole attrito nel 2021, quando le commissioni sono aumentate a causa della crescita esplosiva della catena. Di conseguenza, l'ecosistema Ethereum ha dovuto affidarsi a soluzioni di livello 2 come Polygon e Immutable X per ottenere l'efficienza delle transazioni. Questo è stato anche il momento in cui concorrenti come Solana e Avalanche hanno guadagnato slancio e quote di mercato.

Infine, considerando che le transazioni vengono tolte dalla catena, Lightning Network riduce l'energia necessaria al funzionamento dei nodi. Ciò ha implicazioni significative dal punto di vista della sostenibilità, in quanto il fabbisogno energetico per supportare tali transazioni è inferiore a quello che sarebbe stato necessario se fossero state eseguite sulla rete Bitcoin.

Il Bitcoin è stato oggetto di critiche da parte degli investitori ambientali, sociali e di governance (ESG) che cercano buone credenziali energetiche nei loro investimenti. Riducendo l'impronta energetica e togliendo la maggior parte delle transazioni dalla blockchain di Bitcoin, la Lightning Network aiuta le credenziali di Bitcoin anche dal punto di vista ESG.

Nonostante l'aggiunta di una dimensione chiave per migliorare le capacità della rete Bitcoin nel trilemma della blockchain, la Lightning Network non è priva di aspetti negativi. I problemi principali sono i seguenti.

* costi e attriti per accedere alla rete Lightning
* rischio di controparte durante le transazioni
* mancanza di scalabilità funzionale

Se da un lato la rete Lightning consente di rendere più efficienti le transazioni una volta creati i canali di pagamento tra il mittente e il destinatario, dall'altro lato il processo di creazione del canale è complesso. Gli utenti devono spostare i fondi sulla rete Lightning e inserirli in un canale. Il processo di spostamento dei fondi sulla rete Lightning è costoso.

Una volta che i fondi sono bloccati nel canale e le transazioni tra le due parti iniziano, i fondi sono ancora a rischio. I fondi possono rimanere bloccati nel canale a causa di problemi tecnici oppure la controparte può decidere di chiudere il canale se l'utente va offline e prendere i fondi. Questi rischi offline vengono mitigati dalle torri di guardia e dai fornitori di servizi Lightning. Ma questo aggiunge un vettore di centralizzazione alla rete. Finora non è stata trovata una soluzione infallibile al rischio di controparte a cui un utente è esposto sulla rete Lightning una volta aperto il canale. La rete Lightning ha anche una limitazione più funzionale.

A causa della natura stessa dei canali di pagamento, che sono solo tra due parti, non è senza soluzione di continuità. Di conseguenza, un'azienda che voglia pagare o effettuare transazioni con più controparti dovrà aprire canali per ciascuna di esse e gestirli singolarmente. Per la natura stessa della configurazione, l'azienda sarebbe anche esposta al rischio di controparte su ciascuno di questi canali.

#### 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.

### Sicurezza

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.

#### Immutabilità

Il concetto di immutabilità viene naturalmente ottenuto tramite la combinazione del processo crittografico con il processo di hash. Infatti:

* Ogni transazione verificata dalla rete blockchain viene registrata con un timestamp e incorporata in un "blocco" di informazioni, protetto crittograficamente da un processo di hashing che si collega e incorpora l'hash del blocco precedente e si unisce alla catena come aggiornamento cronologico successivo.
* Il processo di hashing di un nuovo blocco include sempre i meta-dati provenienti dall'output dell'hash del blocco precedente. Questo legame nel processo di hashing rende la catena "infrangibile": è impossibile manipolare o cancellare i dati dopo che sono stati convalidati e inseriti nella blockchain, perché se si tentasse di farlo, i blocchi successivi della catena rifiuterebbero il tentativo di modifica (poiché i loro hash non sarebbero validi). In altre parole, se i dati vengono manomessi, la blockchain si rompe e il motivo può essere facilmente identificato. Questa caratteristica non si riscontra nei database tradizionali, dove le informazioni possono essere modificate o cancellate con facilità.

La blockchain è essenzialmente un registro di fatti in un determinato momento. Nel caso di Bitcoin, questi fatti riguardano le informazioni sui trasferimenti di Bitcoin tra indirizzi. L'immagine sottostante mostra come la somma di controllo dei dati delle transazioni venga aggiunta come parte dell'intestazione, che a sua volta viene sottoposta a hash e diventa la somma di controllo dell'intero blocco.

Perché è importante?

* Integrità completa dei dati - I libri mastri che utilizzano la tecnologia blockchain possono garantire l'intera storia e la traccia dei dati di un'applicazione: una volta che una transazione entra nella blockchain, vi rimane come rappresentazione del libro mastro fino a quel momento. L'integrità della catena può essere convalidata in qualsiasi momento semplicemente ricalcolando gli hash dei blocchi: se esiste una discrepanza tra i dati del blocco e l'hash corrispondente, significa che le transazioni non sono valide. Ciò consente alle organizzazioni e alle autorità di regolamentazione del settore di rilevare rapidamente la manipolazione dei dati.
* Audit semplificato - La possibilità di produrre la storia completa e indiscutibile di un libro mastro transazionale consente un processo di audit facile ed efficiente. Dimostrare che i dati non sono stati manomessi è un vantaggio importante per le aziende che devono rispettare le normative di settore. Alcuni casi d'uso comuni sono la gestione della catena di approvvigionamento, la finanza e la gestione delle identità.
* Aumento dell'efficienza - Il mantenimento di un record storico completo non è solo un vantaggio per la revisione contabile, ma offre anche nuove opportunità di interrogazione, analisi e processi aziendali in generale. FlureeDB, ad esempio, sfrutta il concetto di viaggio nel tempo per le applicazioni aziendali: le query possono essere specificate a partire da qualsiasi blocco, o punto nel tempo, e riprodurre immediatamente la versione del database di quel momento.
  + FlureeDB è un database di tipo blockchain, progettato per archiviare e gestire dati in modo sicuro, trasparente e decentralizzato.
  + FlureeDB utilizza una tecnologia chiamata "blocktree", che combina i vantaggi della blockchain con quelli di una struttura ad albero. Ciò significa che i dati possono essere archiviati in modo sicuro e immutabile, ma con una maggiore flessibilità rispetto alla tradizionale catena di blocchi.
  + Inoltre, FlureeDB offre anche funzionalità come il controllo degli accessi, la gestione dei dati, le query e le analisi avanzate. Ciò consente agli sviluppatori di creare applicazioni decentralizzate e di gestire facilmente i dati in modo sicuro e affidabile.

Questa capacità consente una serie di risparmi di tempo e di costi, tra cui il monitoraggio della provenienza dei principali bug, la verifica di dati specifici dell'applicazione, il backup e il ripristino delle modifiche allo stato del database per recuperare le informazioni. L'immutabilità può rendere irrilevanti i problemi di dati più moderni che affliggono le applicazioni aziendali.

* Prova dell'errore (Proof of Fault) - Le controversie sull'errore nelle aziende sono fin troppo comuni. L'industria delle costruzioni conta 1 trilione di dollari di perdite a causa di controversie non risolte. Anche se la blockchain non eliminerà del tutto questa enorme categoria di procedimenti legali, potrebbe essere sfruttata per prevenire la maggior parte delle controversie relative alla provenienza e all'integrità dei dati (in sostanza, dimostrare chi ha fatto cosa e in quale momento).

Le blockchain, in fin dei conti, sono un meccanismo per rilevare le falsità, non di una magica macchina della verità.

La blockchain non rende i dati intrinsecamente, automaticamente o magicamente veritieri: la sua implementazione si limita a proteggerli crittograficamente in modo che non possano mai essere alterati o cancellati senza conseguenze. Misure come la condivisione dei risultati dell'hash direttamente con le parti interessate (clienti, revisori, ecc.) o la creazione di una rete decentralizzata di nodi di convalida sono un buon complemento all'immutabilità storica fornita dal processo di hashing della blockchain, per garantire una componente di convalida spesso necessaria.

Inoltre: più forti sono le regole di applicazione, più affidabili sono i dati sulla blockchain (esempio: la proof of work di Bitcoin).

* È possibile, ma incredibilmente difficile, ricreare una blockchain con nuovi dati.

Ciò richiede alcune cose: la collusione tra le parti e il ricalcolo completo degli hash. Per una blockchain pubblica come Bitcoin, entrambe le cose sono costose e richiedono un'incredibile quantità di lavoro di calcolo per ri-minizzare i blocchi fino a quando i loro hash possono essere spacciati per validi.

* Quanto più piccola è la cerchia di nodi indipendenti, tanto più facile è ottenere questo risultato.

In termini di svantaggi, avere una storia inalterabile delle transazioni sembra la risposta a molti problemi aziendali moderni - e lo è, per molti versi. Ma cosa succede quando dati sensibili, come gli indirizzi di casa dei dipendenti, vengono accidentalmente pubblicati su una blockchain? Si spera che questo non sia un problema, poiché le decisioni di progettazione standard nella costruzione di ambienti blockchain richiedono una separazione tra informazioni sensibili e informazioni di identificazione personale.

* Se si gestisce una blockchain privata e federata, l'azienda deve convincere le altre parti ad accettare una "biforcazione/fork" della blockchain - dove una blockchain si divide in due percorsi e il nuovo database designato continua. Tutte o la maggior parte delle parti coinvolte in questa blockchain dovranno concordare i termini, compreso il blocco in cui effettuare la biforcazione ed eventuali regole aggiuntive del nuovo database. Se la blockchain è veramente pubblica, è praticamente impossibile rimuovere queste informazioni (anche in questo caso è necessario un hard fork, ma è molto più improbabile che si riesca a convincere le altre parti della rete a conformarsi).
* Per sua natura immutabile, la blockchain è certamente sensibile ad attacchi come il 51 Percent dove un attaccante può acquisire un'enorme potenza di calcolo rispetto agli altri membri della rete. Una blockchain è una forma decentralizzata di rete e nessuna singola entità è al comando. I minatori, tuttavia, possono ancora scrivere la morte per l'immutabilità del sistema blockchain attraverso la creazione di potenza di hashing.

Un altro grosso problema alla blockchain sono i computer quantistici. L'informatica quantistica è considerata una potenziale minaccia per l'immutabilità della tecnologia blockchain. Questo perché i computer quantistici sono potenzialmente in grado di rompere la crittografia che protegge le chiavi private utilizzate per firmare le transazioni su una blockchain.

* In un sistema blockchain tradizionale, le chiavi private vengono utilizzate per firmare le transazioni e dimostrare la proprietà dei beni digitali. Queste chiavi sono protette da algoritmi di crittografia difficili da decifrare con i metodi di calcolo tradizionali. Tuttavia, i computer quantistici sono in grado di eseguire alcuni calcoli molto più velocemente dei computer tradizionali, il che potrebbe rendere possibile la violazione di questi algoritmi di crittografia.
* Se un computer quantistico fosse in grado di rompere la crittografia che protegge una chiave privata, potrebbe potenzialmente consentire a un aggressore di accedere e manipolare i dati memorizzati su una blockchain. Ciò potrebbe compromettere l'integrità e l'immutabilità della blockchain, in quanto le transazioni potrebbero essere alterate o cancellate senza essere rilevate.
* Per mitigare questa minaccia, ricercatori e sviluppatori stanno esplorando modi per creare algoritmi di crittografia resistenti ai quanti, in grado di resistere agli attacchi dei computer quantistici. Questi sforzi includono lo sviluppo di nuove tecniche crittografiche come la crittografia a reticolo e le firme basate su hash, che si ritiene siano più resistenti agli attacchi quantistici. Implementando queste nuove tecniche, potrebbe essere possibile garantire l'immutabilità e la sicurezza dei sistemi blockchain anche di fronte alle minacce dell'informatica quantistica.

#### Usi nelle banche

All’interno delle blockchain si sta sempre più spingendo per meccanismi di verifica degli utenti similari a quelli tradizionali già presenti. Addirittura, si prevede una sua implementazione all’interno di meccanismi di controllo finanziario tradizionale, data la sua natura immutabile, sicura e pubblica.

Possiamo citare ad esempio Il KYC (Know Your Customer), che è un processo attraverso il quale le banche ottengono informazioni sull'identità e l'indirizzo degli acquirenti. Si tratta di un processo di due diligence regolato dalle autorità di vigilanza per verificare l'identità dei clienti. Questo processo aiuta a garantire che i servizi delle banche non vengano utilizzati in modo improprio.

* Le banche sono responsabili del completamento della procedura KYC durante l'apertura dei conti. Le banche sono inoltre tenute ad aggiornare periodicamente i dati KYC dei propri clienti. La procedura KYC può essere manuale, dispendiosa in termini di tempo e ridondante tra le varie istituzioni. La condivisione delle informazioni KYC su Blockchain consentirebbe agli istituti finanziari di ottenere migliori risultati in termini di conformità, aumentare l'efficienza e migliorare l'esperienza dei clienti.
* Il processo di per sé, tradizionalmente, risulta essere ridondante, inefficiente a livello di tempo e ben poco specifico; l'architettura blockchain e la DLT ci permettono di raccogliere le informazioni provenienti da diversi fornitori di servizi in un unico database crittograficamente sicuro e immutabile che non necessita di una terza parte per verificare l'autenticità delle conoscenze. Ciò consente di creare un sistema in cui l'utente dovrà sottoporsi alla procedura KYC una sola volta per verificare la propria identità.

Il processo che implementa la verifica KYC tra banche e blockchain è il seguente:

* Per la procedura KYC, l'utente presenta i documenti a una delle banche in cui vuole ottenere un prestito o utilizzare un altro servizio.
* I singoli partecipanti sono responsabili della raccolta dei dati personali (banche, enti governativi, aziende o utenti stessi) e li memorizzano in una rete decentralizzata.
* La banca controlla e conferma il passaggio del KYC se tutto è normale.
* La banca è responsabile dell'inserimento dei dati dell'utente nella piattaforma blockchain, alla quale hanno accesso altre banche, organizzazioni e strutture statali. Tutte le parti possono controllare e regolare il processo KYC. Il sistema monitorerà le modifiche e gli aggiornamenti dei dati dell'utente e, se qualcuno viola le regole, lo sapranno tutte le parti.
* Quando un utente vuole utilizzare i servizi di un'altra banca, questa seconda banca accede al sistema e conferma così l'identità dell'utente.
* L'accesso ai dati dell'utente sarà basato esclusivamente sul suo consenso. L'utente deve effettuare il login con le transazioni in criptovaluta, cioè utilizzare la chiave privata per avviare l'operazione di scambio di informazioni.

I programmi KYC sono generalmente costituiti da tre componenti: identificazione del cliente, due diligence e monitoraggio continuo.

* Customer Identification Program (CIP)
  + Un programma di identificazione del cliente o "CIP" utilizza dati affidabili e indipendenti per garantire che il cliente sia chi dice di essere. Per le persone fisiche, ciò potrebbe includere il nome legale del cliente, la data di nascita, l'indirizzo e la documentazione di verifica come la patente di guida o il passaporto. Per i clienti aziendali, le licenze commerciali e gli atti costitutivi sono requisiti comuni.
* Customer Due Diligence (CDD)
  + La Customer Due Diligence o "CDD" è una valutazione dei rischi presentati da un nuovo cliente o da un rapporto commerciale. I fornitori di servizi finanziari si avvalgono di controlli di base, indagini sui clienti e analisi della cronologia delle transazioni dei clienti per assegnare valutazioni di rischio che determinano l'intensità del monitoraggio di un conto.
* Monitoraggio continuo
  + Il monitoraggio continuo consiste nell'esame continuo delle transazioni alla ricerca di attività criminali. Quando vengono rilevate attività sospette, i VASP sono obbligati a presentare i rapporti sulle attività sospette (SAR) alla FinCEN o ad altre agenzie di polizia competenti.

Allo stesso tempo vengono fatti dei controlli AML (Anti Money Laundering), quindi antiriciclaggio.

* Il Financial Action Task Force (FATF) stabilisce gli standard per le leggi antiriciclaggio a livello globale. Il FATF ha iniziato a pubblicare linee guida sull'antiriciclaggio delle criptovalute nel 2014 e i responsabili politici delle giurisdizioni membri del GAFI si sono rapidamente attivati; oggi, il FinCEN (Financial Crimes Enforcement Network), la Commissione Europea e decine di altri enti normativi hanno codificato in legge la maggior parte delle raccomandazioni del GAFI in materia di antiriciclaggio delle criptovalute.
* Da qui, il testimone passa ai fornitori di servizi di asset virtuali (VASP), un gruppo che il GAFI definisce come comprendente gli exchange di criptovalute, gli emittenti di stablecoin e, caso per caso, alcuni protocolli DeFi e marketplace NFT. Queste aziende fanno il lavoro pesante per fermare il riciclaggio di denaro impiegando funzionari di conformità antiriciclaggio, richiedendo controlli per conoscere i propri clienti e monitorando continuamente le transazioni di criptovaluta alla ricerca di attività sospette.
* Per valutare i rischi dei clienti e rispettare le normative antiriciclaggio, il KYC (Know Your Customer) è una funzione cruciale. L'identità dei clienti, le minacce che essi rappresentano e le attività finanziarie sono tutti elementi che rientrano nel KYC. Qualsiasi azienda o istituto finanziario deve intraprendere le seguenti azioni per il KYC:
  + Identificare il cliente
  + Esaminare il comportamento del cliente
  + Analizzare il potenziale di riciclaggio di denaro associato a ciascun cliente
* Memorizzando i dati e le informazioni su KYC e AML su un libro mastro decentralizzato, la creazione di una piattaforma AML/KYC abilitata alla blockchain può semplificare le procedure AML/KYC. Le informazioni inserite in un libro mastro blockchain non possono essere modificate o cancellate e sono sempre visibili a tutti i partecipanti alla rete. La gestione dei dati AML/KYC sulla blockchain può quindi aiutare le organizzazioni finanziarie a mantenere i dati senza problemi.
* Le proprietà intrinseche della tecnologia blockchain hanno il potenziale per fermare il riciclaggio di denaro. Ogni transazione effettuata sulla blockchain lascia una traccia cartacea permanente di registrazioni che non possono essere modificate. Di conseguenza, per le autorità è più semplice trovare la fonte originale del denaro.
* La storia completa di ogni transazione può essere monitorata, verificata e registrata in un registro pubblico della blockchain. I minatori di criptovalute e i lettori del libro mastro pubblico vengono avvisati non appena avviene una transazione. La transazione viene immediatamente bloccata se una qualsiasi delle fasi della transazione, tra cui il portafoglio di destinazione, il portafoglio di partenza, il tipo di valuta e l'importo, non viene verificata.
* Anche l'analisi del rischio di riciclaggio di denaro e i meccanismi di segnalazione sono resi possibili dalla blockchain. Consente un'analisi a livello di sistema, invece di concentrarsi solo sui punti di ingresso e di uscita. Inoltre, è tutto automatizzato. Alcuni benefici:
  + Libro mastro immutabile per il monitoraggio normativo
    - In una rete decentralizzata, la Blockchain richiede che ogni utente o nodo convalidi le modifiche. Grazie a questa caratteristica, la rete è estremamente sicura. Ogni nodo mantiene una copia dell'intero libro mastro ed è in grado di confrontare le modifiche e di identificare quelle non approvate. La Blockchain garantisce l'integrità e l'immutabilità dei dati, eliminando le modifiche non autorizzate.
  + Sviluppa la fiducia
    - Il libro mastro incorpora automaticamente la fiducia degli utenti perché è verificabile e immutabile. La blockchain rende incredibilmente semplice e sicuro stabilire la fiducia per qualsiasi transazione, facilitando il trasferimento internazionale di denaro o di altri dati sensibili.
  + Tracciamento delle transazioni
    - Una piattaforma antiriciclaggio basata su Blockchain che incorpora contratti intelligenti automatizza il processo di rilevamento delle frodi del sistema. Gli algoritmi incorporati monitorano continuamente ogni transazione, bloccano istantaneamente quelle che appaiono sospette e generano automaticamente un avviso. Utilizzando la blockchain nell'AML, è possibile ottenere il controllo su tutte le transazioni.

Alcune applicazioni utili della tecnologia blockchain:

* Apertura di un conto bancario
  + Ogni banca deve eseguire la due diligence KYC per aprire un conto bancario e confermare l'identità della persona per valutare il rischio di terrorismo o riciclaggio di denaro. Lavorare con la blockchain presenta molti vantaggi, tra cui l'eliminazione dei silos di dati, la categorizzazione del rischio e i record con data e ora. La piattaforma AML/KYC verifica se i proprietari autorizzati dell'azienda sono persone fisiche o giuridiche quando viene aperto un conto aziendale. Per completare questa verifica, sono necessari i documenti di identificazione personale.
* Richiesta di prestito
  + Secondo la normativa, il KYC è essenziale quando si richiede un prestito. Vengono effettuate valutazione del rischio di criminalità finanziaria, riciclaggio di denaro e affidabilità creditizia. I vari servizi dell'istituto possono accedere rapidamente ai dati del cliente e concludere il processo di richiesta di prestito grazie al libro mastro Blockchain.
* Miglioramenti e correzioni al meccanismo tradizionale KYC
  + Gli istituti finanziari non dovranno più chiedere ai clienti che ritornano i loro documenti per completare il processo di correzione KYC. Il libro mastro sarà utilizzato per memorizzare tutte le informazioni necessarie, compresi documenti, dati, azioni e analisi. Il processo di correzione KYC automatizzato estrae le date di scadenza delle licenze e notifica automaticamente al cliente interessato di caricare documenti più recenti e aggiornati.

# Blockchain: concetti avanzati

Tutti i concetti seguenti fanno parte del cosiddetto Web3, in cui viene data importanza alla rivendicazione della proprietà dei beni digitali, dell’identità autonoma digitale e la decentralizzazione, basandosi su blockchain. Il Web3 si propone di dare una base a tutte le tecnologie esistenti, facendo in modo che il servizio sia costruito e posseduto dagli stessi utenti. Dall’ipertesto (Web1) alla condivisione di contenuti attivi (Web2) alla decentralizzazione. Il paradigma è “lettura, scrittura, proprietà”.

La rete sicura si basa su citati meccanismi di consenso, mentre la protezione dei dati è in mano agli utenti stessi, sostituendo i server con nodi (computer) distribuiti e interagendo con applicazioni decentralizzate chiamate DApp (Decentralized Application), gestite liberamente da una comunità di utenti ma attualmente (per diverse di queste) non funzionanti con i browser tradizionali ed interagendo solo tramite criptovalute, comportando dunque l’apertura di un wallet.

Alcuni dei contenuti della successiva parte riguardano:

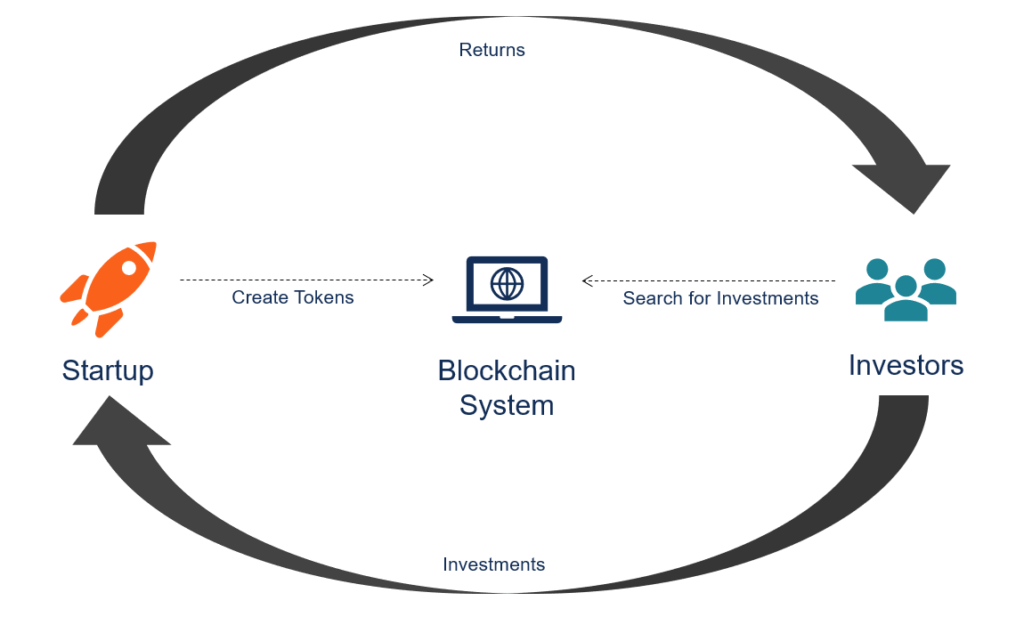
* I *token*, rappresentazioni digitali di un valore o di un'attività che possono essere scambiate e trasferite sulla rete blockchain. I token possono essere utilizzati come moneta digitale, rappresentare asset come titoli azionari, immobili o altre forme di proprietà, o essere utilizzati come strumenti per accedere a servizi o prodotti.
* Gli *smart contract*, software basati su blockchain che permettono di tracciare e gestire lo scambio di criptovalute, effettuando transazioni senza intermediare e in maniera immutabile sulla blockchain
* Le dette *applicazioni decentralizzate (dApp)*, applicazione open source e basate su smart contract, in cui l’utente detiene il pieno controllo delle proprie attività.
* Le *DAO*, organizzazioni che consentono ai creator di avere pari autorità nel contesto di creazione e distribuzione di beni e valori.

## Token

Possiamo definire i token come unità di valore accettate da una comunità e costruite su una blockchain pre-esistente (dunque, non possono essere minati), per esempio quella di Ethereum. Possono essere usati per rappresentare asset fisici come l'oro o l'immobiliare, oppure per rappresentare beni digitali come i dati o i diritti di accesso a servizi. Essendo registrati su una blockchain, sono immutabili e possono essere trasferiti in modo sicuro e trasparente da un proprietario all'altro.

Per utilizzare i token, gli utenti devono prima avere un portafoglio digitale, ovvero un'interfaccia che consente loro di accedere alla blockchain e interagire con essa. Una volta che un utente ha un portafoglio, può ricevere e inviare token. Per ricevere i token, l'utente deve fornire il proprio indirizzo del portafoglio al mittente, che poi invia i token all'indirizzo fornito. Per inviare i token, l'utente deve avere abbastanza token nel proprio portafoglio e deve conoscere l'indirizzo del destinatario a cui inviare i token.

* Viene considerato *asset* in quanto è non riproducibile e non falsificabile, dunque assumendo valore unico. Essi esistono solo in forma digitale ed è tutto ciò che ha valore per un certo stakeholder. Di fatto, viene sottoscritto dalla chiave privata del debitore, poi connesso ad una chiave pubblica del creditore, si ha una sorta di obbligazione a favore del creditore e viene giuridicamente considerato bene mobile.
* In questo contesto parliamo di ICO (Initial Coin Offering) è un evento di raccolta fondi in cui una società o un progetto emette e vende i propri token, utilizzando una blockchain come base tecnologica. Gli investitori possono partecipare all'ICO acquistando questi token con criptovalute o valuta tradizionale.
  + Nel contesto dei token blockchain, gli ICO sono spesso utilizzati come meccanismo di finanziamento per progetti che utilizzano una blockchain come base tecnologica e che intendono emettere un token per rappresentare un valore o un'utilità all'interno del loro ecosistema. L’uso di questa permette di raccogliere fondi eliminando intermediari nel processo di raccolta dei capitali



Riferimento: <https://corporatefinanceinstitute.com/resources/cryptocurrency/initial-coin-offering-ico/>

* I due tipi principali sono:
  + ICO privata
    - Nelle offerte iniziali di moneta private, solo un numero limitato di investitori può partecipare al processo. In genere, solo gli investitori accreditati (istituzioni finanziarie e persone con un elevato patrimonio netto) possono partecipare alle ICO private e una società può decidere di fissare un importo minimo di investimento.
  + ICO pubblica
    - Le offerte iniziali di moneta pubbliche sono una forma di crowdfunding che si rivolge al grande pubblico. L'offerta pubblica è una forma di investimento democratizzata perché quasi tutti possono diventare investitori. Tuttavia, a causa delle preoccupazioni normative, le ICO private stanno diventando un'opzione più praticabile rispetto alle offerte pubbliche.
* Per poterne avviare una, tutto inizia da un *whitepaper*, che permette di descrivere il progetto e il suo stato di avanzamento. Successivamente, occorre identificare gli investimenti e i possibili fondi da acquisire è la creazione dei token, dipendenti dalla piattaforma blockchain utilizzata. Allo stesso tempo, occorre una vasta campagna promozionale e poi avviene la fase di offerta agli investitori.
* Le ICO sono spesso paragonate alle offerte pubbliche iniziali (IPO), un'offerta di nuove azioni da parte di una società privata. Sia le ICO che le IPO consentono alle aziende di raccogliere fondi.

La differenza principale tra le ICO e le IPO è che le IPO comportano la vendita di titoli e sono soggette a normative molto più severe. Una società che vuole condurre un'IPO deve depositare una dichiarazione di registrazione presso la Securities and Exchange Commission degli Stati Uniti e ottenere la sua approvazione. La dichiarazione di registrazione deve includere un prospetto che fornisca i rendiconti finanziari e i potenziali fattori di rischio.

* Le ICO sono in gran parte non regolamentate. Negli Stati Uniti non esistono regolamenti specifici per le ICO. Tuttavia, se una ICO rientra nella classificazione di offerta di titoli, allora ricade sotto la giurisdizione della SEC ed è regolata dalle leggi federali sui titoli. Alcuni Paesi hanno adottato una posizione rigida e hanno vietato completamente le ICO. Tra i Paesi che hanno vietato le ICO vi sono Cina, Nepal, Bangladesh, Macedonia, Bolivia ed Ecuador.
* A livello di vantaggi:
  + Offrono un elevato potenziale di profitto se si è in grado di determinare quale criptovaluta è un buon investimento. Poiché si acquista in anticipo, i prezzi sono spesso più bassi e alcune ICO offrono token a prezzi scontati.
  + Le ICO sono accessibili a tutti. A differenza di alcune IPO, non ci sono restrizioni su chi può investire.
  + È un modo rapido ed efficiente per le start-up di raccogliere fondi.
* A livello di svantaggi:
  + Poiché i progetti di criptovaluta sono volatili, c'è un rischio significativo che il token perda valore o finisca per fallire del tutto.
  + La mancanza di regolamentazione porta a un numero maggiore di truffe e progetti mediocri. Cercare un progetto di qualità tra le prossime ICO può sembrare come cercare un ago in un pagliaio.
  + Di solito è necessaria una certa conoscenza dei portafogli di criptovalute per investire nelle ICO. Per coloro che sono alle prime armi con le criptovalute, spesso è più facile attenersi alle azioni delle criptovalute o alle monete quotate in borsa.
* Ecco alcuni esempi delle principali ICO nel corso degli anni:
  + Ethereum: Molti appassionati di criptovalute erano entusiasti di Ethereum e della sua blockchain programmabile quando si è svolta l'ICO nel luglio 2014. Alla fine ha raccolto 18,4 milioni di dollari ed è diventata la seconda criptovaluta più grande.
  + Cardano (CRYPTO:ADA): Cardano ha migliorato alcuni aspetti di Ethereum e ha avuto un'ICO di successo ancora maggiore. Nel gennaio 2017 ha raccolto 62,2 milioni di dollari. Alla fine entrerà nella top five delle criptovalute per capitalizzazione di mercato.
  + Tezos (CRYPTO:XTZ): Tezos ha raccolto 232 milioni di dollari attraverso la sua ICO nel luglio 2017, ma non è stato un successo completo. Ci sono stati numerosi ritardi nella distribuzione dei token venduti attraverso l'ICO, che hanno portato a un'azione legale collettiva. Tezos ha raggiunto un accordo di 25 milioni di dollari con tutte le parti nel 2020.
  + Dragon Coins (CRYPTO:DRG): Ci sono state molte ICO fallite, e Dragon Coins è uno degli esempi di più alto profilo. Nel marzo 2018 ha raccolto 320 milioni di dollari. Una serie di controversie ha causato un calo quasi immediato del prezzo quando è stata resa disponibile per il commercio pubblico. Nel 2021, la sua capitalizzazione di mercato è scesa sotto il milione di dollari.

### Tipologie di token

* *Payment Tokens,* più comunemente noti come "crypto". Come si può intuire, questi token sono utilizzati per acquistare e vendere beni e pagare le commissioni delle transazioni basate sulla blockchain senza la necessità di un intermediario.
  + Tecnicamente, la maggior parte delle criptovalute potrebbe essere classificata come token di pagamento, a patto che vengano utilizzate come forma di scambio. Più comunemente, però, i token di pagamento non vengono utilizzati per altro che per i pagamenti. Pertanto, non forniscono ai titolari alcuna utilità aggiuntiva oltre al loro valore monetario.
  + Un loro esempio è rappresentato dai token Ethereum o Bitcoin nelle rispettive blockchain.
* *Stablecoins,* che sono è un tipo di criptovaluta agganciata a un bene stabile come il dollaro USA. Lo scopo di una stablecoin è quello di fornire un'alternativa più stabile e meno volatile alle altre criptovalute, come Bitcoin ed Ethereum, che spesso subiscono notevoli fluttuazioni di prezzo.
  + Le monete stabili sono spesso utilizzate come pagamento per beni e servizi e offrono agli utenti commissioni di transazione più basse rispetto ad altre criptovalute e persino ad alcuni popolari servizi di trasferimento di denaro come PayPal. Le Stablecoin sono particolarmente convenienti per l'esecuzione di transazioni internazionali, in quanto le commissioni non aumentano solo perché qualcuno vive dall'altra parte del mondo.
  + Alcuni esempi:
    - Tether (USDT) è forse la più nota stablecoin agganciata al dollaro USA. Tether è stata creata per essere un'alternativa stabile e trasparente alle tradizionali valute fiat da utilizzare in una serie di transazioni di criptovalute.
    - USDC è un'altra stablecoin legata al dollaro USA. È stata progettata per fornire una moneta stabile trasparente e completamente garantita ed è emessa da numerose società, tra cui Circle e Coinbase.
    - Bacon Protocol (bHOME) è un token sostenuto da mutui reali per case e proprietà negli Stati Uniti. Questa moneta può effettivamente crescere di valore man mano che i prestiti vengono rimborsati e gli interessi vengono pagati nel contratto bHome.
* *Defi Tokens,* sono creati appositamente per essere utilizzati in combinazione con piattaforme decentralizzate che operano tramite contratti intelligenti. I token Defi hanno diversi utilizzi, come fornire garanzie per i prestiti, liquidità per il trading e consentire agli utenti di partecipare all'agricoltura di rendimento. Questi token consentono inoltre agli utenti di accedere a informazioni che esistono al di fuori della blockchain, integrando i dati nella rete.
  + Alcuni esempi:
    - Chainlink (LINK) consente agli smart contract di connettersi in modo sicuro a fonti di dati esterne, permettendo di integrare nella blockchain dati ed eventi del mondo reale.
    - Uniswap (UNI) consente agli utenti di utilizzare un modello di market maker automatizzato (AMM) per acquistare e vendere una varietà di criptovalute su uno scambio decentralizzato.
    - Aave (AAVE) consente agli utenti di prestare e prendere in prestito una varietà di criptovalute attraverso una piattaforma decentralizzata di prestiti e prestiti che impiega un modello unico di pool di liquidità.
  + In questo contesto, viene impiegata una tattica di guadagno nota come *yield farming*. Al suo livello di base, lo yield farming consente agli investitori in criptovalute di trarre profitto dai loro investimenti. Lo yield farming è un metodo per guadagnare interessi dalle commissioni di trading depositando unità di criptovaluta in un meccanismo di prestito consentendo consente agli investitori in criptovalute di bloccare le proprie attività in cambio di ricompense.
    - Essa è analoga all'accensione di un prestito bancario. Quando una banca vi presta del denaro, dovete ripagarlo con gli interessi. Lo Yield farming funziona in modo simile, ma questa volta le banche sono investitori in criptovalute come voi.
    - In questo modo, si stabilizza la liquidità e il prezzo del token, allo stesso tempo creando maggiore partecipazione e coinvolgimento sulla rete
* *Governance Tokens,* che sono un tipo di criptovaluta che consente ai titolari di token di votare sulla direzione di un progetto blockchain. Lo scopo principale dei token di governance è quello di decentralizzare il processo decisionale e di dare ai titolari voce in capitolo sulla gestione del progetto.
  + I titolari di token di governance sono di solito più investiti nel successo del progetto, poiché possono guadagnare o perdere di più, a seconda del risultato. I membri della comunità possono utilizzare i token per influenzare direttamente la direzione e le caratteristiche di un protocollo blockchain. In questo modo, è possibile implementare cambiamenti relativi all'interfaccia utente, votare sulle commissioni e sulla distribuzione delle ricompense o persino modificare il codice sottostante di un progetto.
  + Invece, il possesso di token di governance conferisce al titolare il diritto di partecipare alla governance della piattaforma. Ciò può includere il voto sulle proposte di modifica del codice della piattaforma, la determinazione delle modalità di allocazione delle risorse e altre decisioni relative al funzionamento della piattaforma.
  + In molti casi, i token di governance sono utilizzati anche per incentivare la partecipazione al processo di governance: i titolari vengono ricompensati con token aggiuntivi o altri vantaggi per aver partecipato attivamente al processo decisionale della piattaforma.
* *Utility Tokens*, che consentono di acquistare un determinato bene o servizio e conferisce al titolare un diritto di opzione per l’acquisto o somministrazione di cose o per la fornitura di servizi (attuali o futuri). Spesso definiti "coupon digitali" o "redeemable", i token di utilità consentono ai titolari di accedere a prodotti e servizi specifici.
  + Sebbene alcuni dei servizi forniti da un token di utilità siano offerti all'interno dell'ecosistema digitale della blockchain, molti dei benefici potrebbero includere vantaggi della vita reale come prodotti fisici, accesso esclusivo a eventi o persino programmi di mentorship.
  + A differenza degli NFT, i token di utilità sono fungibili, ovvero possono essere scambiati con un altro token dello stesso tipo o con un altro token di pari valore.
  + Alcuni esempi:
    - ApeCoin (APE) è un token di utilità creato appositamente per l'ecosistema Bored Ape Yacht Club. Permette ai possessori di partecipare alle votazioni della governance del progetto, oltre a fornire l'accesso a funzioni riservate ai membri, come giochi, eventi e altri servizi.
    - Decentraland (MANA) è un token utilizzato come pagamento nel mondo virtuale di Decentraland. Viene utilizzato principalmente per acquistare LAND e altri beni virtuali offerti nel gioco.
    - Enjin Coin (ENJ) è un popolare token di utilità sostenuto da miliardi di asset basati sulla blockchain. È noto soprattutto per il suo coinvolgimento nell'ecosistema dei giochi e supporta il commercio di beni di gioco.
* *Security Tokens*, che rappresentano la titolarità di un’attività finanziaria e conferisce un diritto di credito a cui per legge o per contratto possono accedere altri diritti o altre situazioni giuridiche soggettive, come per esempio il diritto di voto che spetta al titolare di un’azione societaria o il diritto alle cedole nelle obbligazioni.
  + Questi token, in sostanza, sostituiscono gli strumenti di investimento tradizionali come le azioni o le obbligazioni, offrendo agli investitori una proprietà frazionata tramite token digitali.
  + Utilizzando la tecnologia blockchain, l'entità definisce i criteri di investimento prima di tokenizzarli e offrirli agli investitori. Non è molto diverso da quando le società distribuivano agli investitori certificati azionari cartacei.
  + La differenza principale è che, poiché questi token vivono sulla blockchain, esiste un record pubblico e immutabile che chiunque può visualizzare e a cui fare riferimento.
  + Alcuni esempi:
    - BCAP è un token per smart contract basato su Ethereum ed è il primo fondo di venture tokenizzato di Blockchain Capital.
    - EXOD è la rappresentazione digitale di un'azione ordinaria di Classe A di Exodus Movement. Questo token consente sia agli investitori al dettaglio che agli investitori accreditati di partecipare alle azioni.
    - VEVU è un token creato appositamente per una società del Wyoming che consente agli investitori internazionali di investire con azioni senza diritto di voto (il che significa che i titolari non hanno diritto di voto per l'elezione degli amministratori).
* *Privacy Coins*, le quali consentono di inviare denaro in modo anonimo. Utilizzando vari metodi, le transazioni completate con le monete privacy rendono difficile per chiunque verificare chi ha inviato o ricevuto il pagamento.
  + Inoltre, i dettagli del pagamento, compresi l'importo e le date della transazione, rimangono anonimi. L'anonimato si ottiene generalmente utilizzando un indirizzo segreto unico e mescolando numerose transazioni in una sola.
  + Alcuni esempi:
    - Zcash (ZEC) è una criptovaluta veloce e riservata che offre agli utenti commissioni ridotte. Utilizza un protocollo di sicurezza per garantire che ogni parte coinvolta sia verificata senza rivelare alcuna informazione sulla parte o sulla rete.
    - Monero (XMR) è utilizzata per pagare beni e servizi in tutto il mondo in tutta riservatezza e con commissioni di transazione estremamente basse.
    - Dash (DASH) è una valuta che consente di inviare denaro a chiunque, ovunque, in modo anonimo e per meno di un centesimo.
* *Exchange Tokens*, tipo di criptovaluta emesso da una borsa. Questi token sono generalmente creati per aumentare la liquidità di un exchange e incentivare le persone a utilizzare la sua piattaforma. Sebbene efficaci, i token di scambio sono uno dei tipi di criptovaluta più volatili sul mercato.
  + I token di scambio sono comunemente utilizzati per pagare le commissioni di transazione sullo scambio. Inoltre, anche se meno comunemente, possono essere utilizzati come token di governance per offrire ai titolari un potere di voto per lo sviluppo futuro della piattaforma.
  + Alcuni esempi:
    - Binance USD (BUSD) è emesso dall'exchange Binance e sostenuto da una riserva di dollari USA. È completamente garantito e soggetto a verifiche trimestrali per garantire l'integrità della riserva. Il BUSD è spesso utilizzato per il trading, i pagamenti, i trasferimenti e come riserva di valore.
    - FTX (FTT) era il token principale dell'exchange FTX prima del suo fallimento. Veniva utilizzato come forma di pagamento con l'ulteriore vantaggio di ridurre le commissioni di trading e di offrire agli utenti diverse altre utilità sulla piattaforma.
    - Crypto.com (CRO) è il token nativo di Crypto.com creato per facilitare le transazioni all'interno della sua blockchain e del suo ecosistema finanziario.
* *Meme Coins,* criptovaluta che si ispira ad alcuni dei meme più popolari al mondo e ad altre barzellette di internet. Questi token di solito non hanno un valore iniziale né sono sostenuti da un bene o da un'utilità sottostante, ma il loro valore è completamente dipendente e derivato dalle comunità che circondano le barzellette.
  + Al di là del sentimento della comunità verso la moneta, non c'è alcun valore da ottenere dal possesso di una moneta meme. Soprattutto se si considera che molte monete meme hanno un'offerta illimitata e non hanno un meccanismo di distruzione, per cui il numero totale di monete in circolazione continua ad aumentare, facendo scendere ulteriormente il valore.
  + Alcuni esempi:
    - Dogecoin (DOGE) è di gran lunga la moneta meme più popolare. È stata originariamente creata per scherzo e ha finito per guadagnare un po' di trazione quando Elon Musk l'ha lanciata. Può essere utilizzata per i pagamenti, tuttavia, nonostante la sua popolarità, rimane estremamente volatile.
    - Shiba Inu (SHIB) è una parodia del Dogecoin. Può essere utilizzata per acquistare beni e servizi nell'ecosistema, ma al di là di questo, è praticamente priva di valore.
    - SafeMoon (SFM) è tecnicamente classificata come una moneta meme a causa della sua comunità online fortificata chiamata SafeMoon Army, tuttavia la società spera che il suo utilizzo come valuta preferita per gli scambi online diventi una realtà.

### Standard per i token

La creazione di token usa le blockchain per trasmetterli in maniera sicura senza intermediari ed utilizza gli smart contract per crearne di nuovi.

La loro creazione segue alcuni standard, di seguito listando i principali:

* ERC-20, uno standard tecnico utilizzato per creare e gestire token su blockchain Ethereum. La sigla "ERC" significa "Ethereum Request for Comment" e il numero "20" rappresenta l'identificatore univoco dell'implementazione del protocollo. Lo standard generale dei token offre la funzionalità di base per il trasferimento dei token, oltre a supportare l'approvazione dei token per le spese da parte di altre terze parti della catena.
* I token ERC-20 sono token fungibili e Le aree di applicazione più popolari sono le Stablecoin, i token di governance e le ICO. Esso richiede una singola operazione per ogni transazione, senza verifiche KYC (Know Your Customer), con uno smart contract comune e richiedendo più spazio; esso trasferisce 1/2 token alla volta.
* I token ERC-20 hanno le seguenti funzionalità standard:
  + Saldo del token: ogni account può avere un saldo di token associato ad esso.
  + Trasferimento di token: i token possono essere trasferiti da un account all'altro.
  + Approvazione di token: gli account possono approvare altri account per prelevare un determinato numero di token.
  + Ottenere il saldo di token di un account: gli account possono controllare il saldo di token di un altro account.
  + Ottenere il totale di token disponibile: gli account possono controllare il numero totale di token in circolazione.
* In questo standard sono presenti 9 regole, di cui 6 obbligatorie e 3 opzionali.
  + Regole e norme obbligatorie
    - allowance (controllo della transazione e ne permette l’esecuzione se il bilancio è sufficiente)
    - approve (approvazione del contratto per ottenere soldi)
    - transferFrom (per automatizzare alcune transazioni e renderle fisse)
    - transfer (trasferimento dei token ad un altro indirizzo)
    - balanceOf (numero totale di token che un indirizzo ha)
    - totalSupply (numero totale di token da creare)
  + Regole/standard opzionali
    - Token Name
    - Decimal (massimo: 18)
    - Immagine che contiene testo

      Descrizione generata automaticamenteSymbol

L’utilizzo di ERC20 permette lo sviluppo delle DApp standard, rendendo l’implementazione semplice per i blockchain developer, offrendo un protocollo di ampia adozione, personalizzabile e con ampia liquidità. Per contro. Tuttavia, possono essere soggetti a problemi di sicurezza (sfruttando ad esempio il bug sulla funzione *transfer* per cui il recipiente non riceve notifica dei fondi e se non riceve il token, nessuno può usarlo), richiedendo maggiore centralizzazione e regolamentazione per utilizzo.

Occorre usare per il bug di prima la combinazione "approve" e "transferFrom". Se si inviano token a uno smart contract usando la funzione "transfer", si vedrà una transazione riuscita, ma il contratto non riceverà mai i token. Questo bug brucia i token in modo permanente e non è possibile recuperarli.

A livello di codice si presenta come a lato.

Riferimento: <https://www.leewayhertz.com/erc-20-vs-erc-721-vs-erc-1155/>

* ERC-721, specificamente legato agli NFT. A differenza dei token ERC-20, che sono intercambiabili con altri token dello stesso tipo, i token ERC-721 sono unici e non possono essere sostituiti uno con l'altro. Ogni token ERC-721 rappresenta un oggetto digitale unico e può essere utilizzato per rappresentare qualsiasi cosa di valore, come ad esempio un'opera d'arte, un oggetto collezionabile, un immobile o un diritto d'autore.
  + Gli ERC-721 sono utilizzati principalmente in applicazioni decentralizzate (dApp) che richiedono la proprietà univoca e la trasferibilità di oggetti digitali, come i mercati NFT, i giochi blockchain e le piattaforme di condivisione di contenuti.
  + Si noti che ogni NFT ha una variabile uint256 nota come *tokenId*. Pertanto, per ogni contratto EBR-721, la coppia indirizzo del contratto - tokenId uint256 deve essere unica.
  + Inoltre, le dApp devono disporre di un "convertitore" per regolare il processo di ingresso e uscita degli NFT. Ad esempio, il convertitore considera il tokenId come input e produce token non fungibili come un'immagine di zombie, uccisioni, oggetti da collezione del gioco, ecc.

A livello di codice si presenta così:

Immagine che contiene testo

Descrizione generata automaticamente

Riferimento: <https://www.leewayhertz.com/erc-20-vs-erc-721-vs-erc-1155/>

* ERC-1155­, combinando le capacità di ERC-20 e ERC-720, Witek Radomski (CTO di Enjin) ha introdotto un token standard onnicomprensivo per gli smart contract di Ethereum. Si tratta di un'interfaccia standard che supporta lo sviluppo di token fungibili, semi-fungibili, non fungibili e altre configurazioni con un contatto intelligente comune. Questa permette operazioni multiple in una singola transazione, richiedendo un solo smart contract per infiniti token
  + Ora è possibile soddisfare tutte le esigenze di sviluppo dei token e affrontare i problemi utilizzando un'unica interfaccia, rendendo ERC-1155 un vero e proprio cambiamento. L'idea di questo standard unico per i token è stata quella di sviluppare una robusta interfaccia per smart contract che rappresenti e gestisca diverse forme di token ERC.
  + Un altro aspetto positivo di ERC-1155 è che migliora la funzionalità complessiva dei precedenti standard di token ERC, rendendo l'ecosistema Ethereum più efficiente e scalabile. Questo rappresenta quindi un mezzo intermedio per poter usufruire di tutti i token, fungibili e no.

Immagine che contiene testo

Descrizione generata automaticamente

Riferimento: <https://www.leewayhertz.com/erc-20-vs-erc-721-vs-erc-1155/>

Ulteriori standard da citare:

* ERC-165, uno standard di interfaccia che definisce un metodo per determinare se un contratto supporta determinate funzionalità. Questo standard consente ai contratti di verificare se un altro contratto implementa determinate funzioni e in tal modo consentire loro di interagire con esso in modo appropriato. ERC-165 utilizza l'identificatore dell'interfaccia (Interface ID) per consentire ai contratti di identificare le funzionalità supportate da un altro contratto.
  + Si tratta in realtà di uno standard per un metodo, anziché per i token. Tuttavia, è importante per un altro standard di token, ERC721, che non può essere implementato senza di esso.

Uno smart contract deve interagire con i token crittografici. Anche se tutti i contratti possono interagire con i token ERC 20, è diverso da altri standard ERC per i token, come ERC 721. I contratti intelligenti devono contratti intelligenti devono implementare interfacce specifiche per interagire con i token che seguono altri standard.

* + Ora, la comunità di sviluppo di Ethereum ha bisogno di sapere quali interfacce implementa uno smart contract ed è necessario pubblicare queste informazioni. Questo perché devono sapere in quali modi possono interagire con quel contratto.

Non esisteva un metodo standard per rilevare le interfacce utilizzate da uno smart contract e per pubblicarle. L'ERC 165 standardizza un metodo per questo, oltre a standardizzare l'identificazione delle interfacce.

* ERC-223, che non si tratta di un token digitale onnicomprensivo, ma fornisce una soluzione ad alcuni dei problemi di UX associati ad altri token ERC. In molti casi, le monete vengono inviate all'indirizzo sbagliato del portafoglio o a uno smart contract, con il risultato di essere perse per sempre.
  + Alcuni sviluppatori cinici potrebbero dire che gli utenti finali possono essere incolpati di aver inviato i token all'indirizzo sbagliato, ma questo potrebbe limitare l'accettazione da parte del pubblico. L'interfaccia poco intuitiva può allontanare le persone che non sono tecnicamente preparate.
  + Una caratteristica fondamentale della proposta ERC-223 è che essenzialmente dice agli utenti quando inviano token a indirizzi errati di contratti smart e li annulla. In cambio del pagamento del gas, gli utenti risparmiano il loro Ethereum. In cambio del pagamento della benzina, gli utenti salvano la loro piattaforma Ethereum. Il software offre funzionalità UX di facile utilizzo che proteggono gli utenti dai fallimenti dei fondi, compatibilità con lo standard dei token ERC-20 e costi operativi inferiori a quelli di Ethereum.
  + Gli sviluppatori possono accettare o rifiutare i token che arrivano agli indirizzi dei loro smart contract. Specifica le funzioni che un contratto può codificare in modo che se non può accettare i token, il trasferimento fallisce. Nessun token lo utilizza e gli scambi di criptovalute potrebbero non essere preparati per questo standard.
* ERC-621, estensione dell'ERC 20, questo standard consente di aumentare o diminuire la fornitura totale di token utilizzando due funzioni, "increaseSupply" e "decreaseSupply". La proposta raccomanda che solo il proprietario del contratto o gli utenti fidati possano utilizzarle.
  + Le criptovalute sono denaro matematico, a differenza delle valute fiat in cui le banche centrali possono aumentare o diminuire l'offerta. L'offerta totale di token è uno dei tanti fattori che determinano l'apprezzamento dei token e influisce sull'economia di un token.
  + Questa proposta è una bozza e dobbiamo vedere se la comunità di Ethereum la implementerà, visto l'ampio impatto.
* ERC-725, uno standard di identità basato su Blockchain sviluppato da Fabian Vogelsteller, lo sviluppatore del noto standard ERC-20. Gli smart contract definiti da ERC-725, che definisce i contratti proxy, possono avere più chiavi ed essere associati a diversi smart contract. Individui, macchine e oggetti possono essere definiti con smart contract di identità.
  + La governance e la reputazione decentralizzate sarebbero facilitate da uno standard di identità aperto e portatile. Le persone dovrebbero poter utilizzare la propria identità su più piattaforme e applicazioni.
* ERC-777, standard proposto che include una funzione per identificare la ricezione dei token e avviare uno smart contract subito dopo la prima transazione. Se da un lato riduce l'overhead delle transazioni, dall'altro consente all'utente di rifiutare i token in arrivo da un indirizzo inserito nella blacklist. L'inserimento di un indirizzo nella lista nera può essere dovuto a vari motivi, come hacking o attività illegali. La possibilità di rifiutare il pagamento da un tale indirizzo migliora la posizione di sicurezza di una DApp Ethereum.
  + L'ERC 777 mantiene tutti i punti di forza dell'ERC 20. OpenZeppelin (libreria per lo sviluppo di smart contract sicuri) ha già implementato ERC777 per costruire, automatizzare e gestire applicazioni decentralizzate.
* ERC-827, che permette il trasferimento di token a terzi per spenderli. Si tratta di un'altra estensione dell'ERC 20, ma intende risolvere il problema che l'ERC 223 cerca di risolvere, in modo migliorato. Se questo standard viene implementato, il titolare di un token può trasferire i token e allo stesso tempo approvare che una terza parte li spenda.
  + Con questo standard ERC, i portafogli e gli scambi possono riutilizzare i token, perché entrambe le parti concordano su criteri specifici per la spesa di una terza parte per un importo dinamico. La comunità di Ethereum non l'ha ancora implementato.
* ERC-865, uno standard di interfaccia che definisce un metodo per ridurre i costi di transazione sui token Ethereum. Questo standard consente agli utenti di pagare i costi di transazione in token invece che in Ether, il che può ridurre significativamente i costi di transazione. ERC-865 definisce una serie di funzioni per effettuare pagamenti e consente ai contratti di delegare i costi di transazione agli utenti che effettuano le transazioni.
  + Quando un utente nuovo alle criptovalute cerca di trasferire i token basati su Ethereum, scopre improvvisamente di dover pagare le commissioni dei minatori in Ether. Questo aumenta l'attrito per l'utente.
  + Tra gli standard ERC proposti dagli sviluppatori della comunità di Ethereum, l'ERC 865 intende semplificare la vita dei nuovi utenti di criptovalute.
* ERC-884, uno standard di interfaccia per token Ethereum che consente la creazione di token non fungibili (NFT) che rappresentano il possesso di beni fisici o digitali. Questo standard definisce un insieme di funzioni per creare, trasferire e gestire i NFT, consentendo a diverse applicazioni di interagire con questi token in modo standardizzato.
  + Per rispettare le normative, ERC 884 include anche quanto segue:
    - Verifica dell'identità e whitelisting obbligatorio dei titolari di token;
    - La società può preparare un elenco degli azionisti in base ai requisiti normativi;
    - Registrazione delle informazioni mandato dei regolatori;
    - Registrazione del trasferimento di azioni in base ai requisiti normativi;
    - Solo il valore intero dei token, cioè nessun valore parziale;
    - Gli azionisti che hanno perso le chiavi private o i token devono recuperarli a un nuovo indirizzo.
  + L'implementazione dell'ERC 884 richiede un database fuori dalla catena per vari requisiti "Know Your Customer" (KYC). Si tratta ancora di una bozza di proposta

### Fungible Tokens

I token fungibili sono criptovalute che presentano tutte le caratteristiche standard degli asset fungibili. In altre parole, queste criptovalute dovrebbero essere non uniche, divisibili e avere un chiaro valore di mercato. Non dovrebbe essere difficile per i trader determinare il valore dei loro token fungibili o fare trading con essi sugli scambi di criptovalute.

#### Tipologie

Alcune delle tipologie listate di seguito sono già state citate sopra, pertanto qui sintetizzate:

* Stablecoin: è un tipo di token fungibile che mira a mantenere un valore stabile, spesso agganciato a una valuta tradizionale o a un altro asset stabile. Gli stablecoin possono essere utilizzati come riserva di valore o come mezzo di scambio, senza le fluttuazioni di prezzo tipiche di altre criptovalute.
* Utility token: è un tipo di token fungibile che conferisce al possessore il diritto di accedere a un servizio o a una funzionalità specifica all'interno di una piattaforma o di un'applicazione. Questo tipo di token può essere utilizzato come forma di pagamento all'interno della piattaforma che lo emette.
* Security token: è un tipo di token fungibile che rappresenta un investimento in un'azienda o in un progetto. A differenza degli utility token, i security token sono considerati titoli finanziari e sono soggetti alle normative sui mercati finanziari.
* Asset token: è un tipo di token fungibile che rappresenta la proprietà di un asset fisico o di un bene virtuale. Gli asset token possono rappresentare, ad esempio, l'acquisto di un bene immobiliare o di una quota di una società.
* Commodity token: è un tipo di token fungibile che rappresenta la proprietà di una materia prima, come oro, argento, petrolio, ecc. Questo tipo di token permette agli investitori di acquistare una quota di un bene fisico senza la necessità di possederlo fisicamente.

Ora passiamo ad altre tipologie di token fungibili:

* CDBC (Central Bank Digital Currency), utilizzabile qualora emessa da una banca centrale per accumulare valore ed effettuare pagamenti, vista come valuta fiduciaria affinché possa essere utilizzata (meglio in futuro) come sistema accessibile e disponibile da tutti i cittadini. Esse vengono supportate dai governi del paese, dando la possibilità di effettuare trasferimenti diretti; per contro, non hanno un valore pienamente stabile (dipendente dal mercato, non dal contesto stesso del paese) ed occorre chiaramente un wallet per la gestione delle chiavi e dei propri dati.
* Branded currency, che può essere definita come - una riserva di valore e un mezzo di scambio per beni e servizi di un marchio o di un commerciante specifico; ciò include qualsiasi forma fisica o digitale di pagamento da parte di un commerciante o di un marchio, come coupon, punti fedeltà e carte regalo. Vengono viste come un mezzo di connessione tra utenti reali e brand, sia come mezzo di maggiore connessione verso di lui che come ulteriore trasformazione digitale
  + Le criptovalute di marca cercano di risolvere i problemi di rottura e di valore inutilizzato all'interno dell'economia delle valute di marca tradizionali, eliminando gli attriti e gli altri punti dolenti inerenti all'infrastruttura attuale
  + Tuttavia, alcune valute di marca come i punti e le carte regalo sono ancora considerate pagherò e non sono esplicitamente garantite. Possono corrispondere a un valore in dollari, ma non sono direttamente garantite dai dollari associati.
  + Aziende come Walmart e Facebook stanno esplorando questo settore in quanto l’accesso alle blockchain potrebbe consentire a circa 1.7 miliardi di persone di accedere ai sistemi finanziari, permettendo direttamente agli utenti di utilizzare una valuta considerata come asset facilmente integrabile in molti altri sistemi reali

### NFT (Non Fungible Tokens)

I token non fungibili (NFTs) non possono essere interscambiati in quanto costituiscono la rappresentazione digitale di oggetti unici o rari ed hanno valore di certificato di proprietà digitale. Gli NFT non possono essere scambiati o negoziati come gli altri token crittografici, poiché sono tutti tecnicamente unici, quindi hanno un valore proprio.

* Un NFT può rappresentare una serie di cose sia nel regno fisico che in quello digitale. Arte, musica, oggetti di gioco, biglietti e naturalmente oggetti da collezione sono tutti esempi di ciò che un NFT può rappresentare in forma digitale. Essi possono essere aggiornati in qualsiasi momento, aggiungendo nuove caratteristiche in ogni momento.
* I non fungible-token vengono comunemente utilizzati per la gestione dell’identità digitale, i progetti di tracciabilità (in questo caso si parla di digital twin) e dell’automazione dei processi di supply chain, il voto elettronico, i collezionabili intesi come bene nei giochi online.

Il processo di pubblicazione di un token unico su una blockchain viene definito come minting (conio), generalmente utilizzato per descrivere il processo di creazione di un NFT. Si usa anche per descrivere l'atto di acquistare un token non fungibile direttamente da uno smart contract. Il processo impiega 5 minuti per un singolo NFT fno ad alcune settimane per un intera collezione tramite uno smart contract

* Come creatore, si conia un NFT per renderlo disponibile per la vendita ad altri. In questo modo, si pubblica un singolo NFT oppure una collezione di essi.
* Come consumatore, si può coniare un NFT da un contratto, che viene poi rivelato dopo l'acquisto. Da questo punto di vista, si intende comprare un NFT, permettendo di diventare il possessore unico della stessa

Prima di effettuare il minting, è necessario considerare:

* La piattaforma blockchain opportuna, affinché la supporti e sia popolare, oltre che compatibilità con la stessa. Si realizza un processo definito come *wrapping*, per il quale la NFT ha funzionalità economiche, di prestito, anti-frode e protetto da svalutazione. Questo permette di spostarle tra blockchain diverse.
* I costi di creazione, da un punto di vista di sicurezza, efficienza e funzionalità.

Per effettuarlo, occorre:

* Creare un file digitale che verrà pubblicato sulla blockchain. Questo file può essere un'immagine, un video, un audio o una combinazione di questi. Tuttavia, è bene tenere presente che ci sono limitazioni di upload.
* Comprare alcune cripto, in quanto per creare un asset digitale è necessario utilizzare la criptovaluta per pagare le spese di transazione relative alla blockchain. Ogni blockchain utilizza la propria criptovaluta nativa, pertanto è necessario assicurarsi di acquistare la valuta corretta per la blockchain in uso.
* Usare un wallet di qualsiasi tipo
* Pubblicare l’asset nella blockchain; è possibile crearlo anche gratuitamente, eseguendo il minting solo quando l’oggetto viene acquistato e il compratore pagherà il gas necessario per pubblicarlo su di essa.

L'acquisto di un NFT presso la zecca (at mint) presenta molti vantaggi e svantaggi. A livello di vantaggi:

* Profitto dall'essere tra i primi ad acquistare: Può essere vantaggioso essere tra i primi ad acquistare nuovi token. Infatti, i primi investitori possono ottenere gli NFT al prezzo più basso possibile. Di conseguenza, siete in una posizione eccellente per aumentare il rendimento del vostro investimento in NFT.
* Ottenere un accesso esclusivo alle DAO e altri vantaggi di essere i primi: l'acquisto di un NFT può darvi un vantaggio nell'aspetto della comunità. Ad esempio, i casi in cui gli NFT possono fornire ai possessori di token l'ingresso nella DAO del progetto possono far sì che gli investitori ricevano delle partecipazioni nella direzione in cui il progetto potrebbe andare.

A livello di svantaggi:

* Rischio di diminuzione del valore dopo il conio: Il mercato speculativo è uno dei motivi principali per cui il conio di nuovi NFT comporta un rischio significativo. Non c'è alcuna garanzia che il valore del vostro prodotto aumenti nel tempo. Tra l'altro, potreste anche trovarvi di fronte a circostanze in cui il prezzo scende vertiginosamente subito dopo il conio.
* Elevate commissioni di gas: Ci sono momenti in cui il prezzo d'ingresso potrebbe salire notevolmente a causa dell'aumento dell'attività della rete. A volte, ci possono essere troppe persone contemporaneamente che cercano di ottenere un posto nella zecca. Di conseguenza, la tassa sul gas può aumentare rapidamente.

Il processo di distruzione è definito come burning e, come già visto, si intende inviare il token ad un indirizzo non spendibile che nessuno può accedere, pagando una tassa di *gas*.

La principale classificazione dei tipi di NFT si riferisce alle categorie generali. I tre tipi comuni di NFT comprendono:

* Originale o copia di un'opera, documentata su una rete blockchain o DLT
* NFT nativi digitali, che hanno diritti di proprietà sull'opera che li costituisce
* metadati NFT, che prevede che l'NFT fornisca la rappresentazione della proprietà per i file di metadati relativi a Internet.

I tipi comuni di token non fungibili offrono un'ampia descrizione dei criteri utilizzati nella classificazione degli NFT. Nel caso degli NFT originali, essi sono creati su una rete blockchain e gli NFT rimangono sulla rete blockchain. I NFT nativi digitali sono i beni che comportano l'emissione di NFT a più persone con diritti di proprietà del bene. I metadati dell'NFT sono un'altra indicazione importante per la classificazione dei token non fungibili, in quanto si tratta essenzialmente di un collegamento ai metadati dell'NFT. Di conseguenza, non si ottiene la proprietà dell'NFT, ma solo i diritti di utilizzo.

#### Tipologie

Le voci di spicco di un elenco di token non fungibili sono le seguenti:

* Oggetti da collezione (collectibles)
  + Il principale esempio di NFT è emerso con lo sviluppo dei Cryptokitties, che sono oggetti da collezione online. Di fatto, i Cryptokitties sono il primo caso di utilizzo di NFT. È interessante notare che nel 2017 i Cryptokitties sono diventati così popolari da congestionare la rete Ethereum. I Cryptokitties sono una delle aggiunte più sorprendenti alla lista dei token non fungibili nella categoria degli oggetti digitali da collezione. Si tratta fondamentalmente di gattini digitali con caratteristiche distinte che li rendono più popolari e favorevoli di altri.
* Opere d'arte (artworks)
  + Anche le opere d'arte sono un altro candidato importante per i NFT. I tipi comuni di gettoni non fungibili in questo settore si riferiscono all'arte programmabile, che presenta una combinazione unica di creatività e tecnologia. Attualmente sono in circolazione molte opere d'arte in edizione limitata che possono essere programmate a determinate condizioni. L'uso di oracoli e contratti intelligenti potrebbe aiutare gli artisti a creare immagini rappresentate su reti blockchain. Le NFT per l'arte digitale hanno anche incoraggiato le possibilità di partecipazione dell'industria artistica tradizionale.
  + La tokenizzazione di beni e opere d'arte del mondo reale potrebbe contribuire a incoraggiare l'adozione delle NFT. La possibilità di combinare blockchain e IoT potrebbe offrire prospettive interessanti per la scansione di un codice o di un adesivo sui beni. I tipi di NFT nelle opere d'arte potrebbero garantire che gli utenti possano facilmente registrare la proprietà di opere d'arte reali su una rete blockchain. Successivamente, gli utenti potrebbero anche scoprire la storia completa di un'opera d'arte, come i precedenti proprietari e i prezzi per cui è stata venduta in passato.
* Biglietti per eventi
  + Un'altra promettente aggiunta tra i tipi di NFT riguarda i biglietti per eventi. Questi tipi di NFT consentono alle persone che partecipano a eventi come festival musicali e concerti di verificare la loro identità e i loro biglietti. I gestori degli eventi potrebbero coniare un numero specifico di biglietti NFT su una piattaforma blockchain selezionata. I clienti potrebbero acquistare i biglietti attraverso un'asta e conservarli nei loro portafogli, facilmente accessibili attraverso i dispositivi mobili.
* Musica e media
  + Anche il settore della musica e dei media sta sperimentando le NFT, dando vita a un'altra categoria di NFT. È possibile collegare i file musicali e multimediali agli NFT, consentendo così a un individuo con un vero diritto di proprietà di accedere ai file. Le due principali piattaforme che aiutano gli artisti a coniare le loro canzoni come NFT sono Rarible e Mintbase.
  + Mentre gli artisti ottengono il vantaggio di raggiungere direttamente i propri follower e il nuovo pubblico, gli ascoltatori ottengono un'esperienza premium. Il senso di esclusività nell'acquisto di musica NFT è uno dei motivi principali per cui i dischi in vinile vintage sono stati infusi. La crescita dei NFT musicali nell'elenco dei gettoni non fungibili potrebbe offrire prospettive affidabili per affrontare i problemi della pirateria musicale e degli intermediari.
* Videogiochi (Gaming)
  + I tipi comuni di gettoni non fungibili nel settore dei giochi si concentrano principalmente sugli oggetti di gioco. I NFT hanno suscitato un grande interesse tra gli sviluppatori di giochi. Possono offrire la funzionalità di record di proprietà per gli oggetti di gioco, favorendo così la crescita delle economie di gioco. Ma soprattutto, gli NFT nel settore dei giochi si concentrano sull'introduzione di un'ampia gamma di vantaggi per i giocatori.
  + Mentre gli oggetti da collezione in-game erano requisiti comuni per una migliore esperienza di gioco, gli NFT hanno il potenziale per cambiare il loro valore. Gli oggetti di gioco come NFT potrebbero facilmente aiutare a recuperare denaro vendendoli al di fuori del gioco. D'altra parte, gli sviluppatori di giochi o i creatori che emettono NFT potrebbero guadagnare una royalty per ogni vendita di oggetti nel mercato aperto.
* Asset del mondo reale
  + Anche se non è possibile trovare molti tipi di NFT che fungono da gettoni per oggetti del mondo reale, i progressi nel campo degli NFT possono far sì che ciò accada. Ad esempio, molti progetti NFT si stanno attualmente concentrando sulla tokenizzazione di beni immobili e di beni di lusso. Gli NFT sono fondamentalmente atti di proprietà e possono introdurre la flessibilità di acquistare un'auto o una casa con un atto di proprietà NFT. Pertanto, gli NFT che rappresentano beni del mondo reale possono sfruttare le opportunità offerte dalla prova crittografica della proprietà.
* Identità
  + Una delle caratteristiche fondamentali dei token non fungibili è la scarsità. Ogni NFT è unico e non può essere scambiato con nessun altro token. Nel caso degli NFT di identità, il funzionamento è simile a quello degli NFT di biglietti per eventi. Possono fungere da identificatori unici e quindi da supporto affidabile per i sistemi di gestione dell'identità.
  + Le applicazioni comuni degli NFT basati sull'identità possono essere evidenti nelle certificazioni e nelle licenze. La creazione di certificazioni e licenze e di NFT per dimostrare e verificare i dati di un individuo potrebbe cambiare il settore della gestione dell'identità. Inoltre, gli NFT basati sull'identità potrebbero anche garantire che gli individui possano conservare le prove della loro identità senza rischiare di perderle.
* Memes
  + Il progresso più significativo nel settore delle NFT negli ultimi tempi è la vendita di meme come NFT. Oltre a far parte della cultura popolare e a essere immediatamente preferiti dagli utenti di Internet, i meme sono stati associati alle NFT. La vendita di meme come NFT mostra il potenziale dei creatori di meme unici di partecipare a un ecosistema futuristico in evoluzione.
* Nomi di dominio
  + Questi ultimi sono diventati popolari di recente. I servizi di nomi di dominio decentralizzati, come Unstoppable Domains e Ethereum Name Service (ENS), sono i principali esempi di NFT di nomi di dominio. ENS può aiutare a tradurre indirizzi utente lunghi e complessi in un'esperienza flessibile e amichevole per gli utenti, con una curva di apprendimento più semplice

## Tokenizzazione

La tokenizzazione è il processo di rappresentazione di un bene o di un'attività in forma digitale attraverso l'emissione di un token su una blockchain. In altre parole, si tratta di convertire un bene fisico o immateriale in un asset digitale che può essere negoziato e scambiato in modo decentralizzato.

* Fondamentalmente, i token blockchain forniscono una rappresentazione digitale della proprietà completa o condivisa di qualsiasi entità con un valore specifico. Le applicazioni comuni dei token blockchain sono evidenti nei pagamenti e nel regolamento delle transazioni tra i partecipanti. I token rappresentano anche la proprietà di più parti per beni indivisibili come opere d'arte o video musicali. Inoltre, i token consentono un più facile scambio di proprietà di beni indivisibili attraverso una rete blockchain.
* La combinazione tokenizzazione - blockchain potrebbe aprire nuove prospettive per l'ottimizzazione dei processi aziendali, che includono più partner, e l'introduzione di nuovi modelli di business. Secondo IDC, il mercato globale degli asset tokenizzati raggiungerà una valutazione di 500 miliardi di dollari. Sebbene si possano notare promettenti opportunità per la tokenizzazione di asset sulla blockchain, il concetto di token non è nato qui.
* Infatti, i token sono stati utilizzati come meccanismo unico di sicurezza dei dati nei servizi finanziari per salvaguardare informazioni riservate come numeri di carte di credito, informazioni di identificazione personale e rendiconti finanziari.

Esistono diversi tipi di asset da considerare, i quali saranno poi successivamente convertiti in token:

* *Beni immateriali (intangibles)*
  + I beni immateriali esistono solo in base a precedenti legali, senza alcun oggetto fisico che li rappresenti. Esempi di beni immateriali sono i diritti d'autore e i brevetti. Quando si desidera tokenizzare i beni immateriali, è importante assicurarsi che il modello di trasferimento dei beni della rete blockchain sia uguale a quello del mondo reale. I beni immateriali sono facili da convertire in token senza problemi di stoccaggio o spedizione. Al contrario, le differenze giurisdizionali potrebbero creare profonde difficoltà per il trasferimento di token che rappresentano beni immateriali.
* *Fungible Assets (asset fungibili)*
  + I beni fungibili sono quelli che possono essere sostituiti da un bene simile. Gli esempi più comuni di beni fungibili sono il grano o l'oro. Convertire i beni fungibili in gettoni è più facile, in quanto è possibile dividerli facilmente in unità più piccole. Inoltre, un gettone può servire come rappresentante di un gruppo di beni fungibili, come un mucchio d'oro. L'algoritmo di tokenizzazione per gli asset fungibili deve anche includere un livello di astrazione. Inoltre, un insieme di token è correlato a una collezione di componenti di asset intercambiabili.
* Un asset fungibile ha due caratteristiche:
  + È intercambiabile, in quanto ogni unità ha lo stesso valore di mercato e validità
  + È divisibile, in quanto può essere suddivisa nel numero di cifre decimali che sono state configurate al momento della sua emissione. Ogni unità avrà lo stesso valore e la stessa validità.
* *Non-fungible Assets (asset non fungibili)*
  + Gli asset non fungibili sono quelli che non possono essere scomposti in pezzi più piccoli. La tokenizzazione aiuta a scomporre gli asset non fungibili in azioni digitali, che possono essere scambiate completamente o in modo limitato. L'esempio di tokenizzazione di opere d'arte e immobili mostra le possibilità di conversione di beni non fungibili in token.
  + La conversione di opere d'arte in token inizia con l'introduzione di una firma digitale immutabile. La firma digitale o token fornisce una rappresentazione dell'opera d'arte mantenendo l'unicità. Successivamente, è possibile suddividere il token in sub-token più piccoli che possono essere firmati digitalmente. È quindi possibile vendere i token come azioni dell'opera d'arte originale.
* Un asset non fungibile ha tre caratteristiche:
  + Non intercambiabili: Gli NFT non possono essere sostituiti con token dello stesso tipo, perché ogni token rappresenta un valore unico.
  + Non divisibili: Gli NFT non sono tipicamente divisibili, anche se gli F-NFT (fractional NFT, un inter NFT che è stato diviso in frazioni più piccole permettendo a varie persone di prendere proprietà dello stesso NFT. Questi offrono la proprietà frazionaria degli NFT, come nel caso di costose opere d'arte o immobili commerciali.).
  + Unico: Ogni token si differenzia da un altro token dello stesso tipo e possiede informazioni e attributi unici.

### Cosa tokenizzare, tipi e benefici

Le possibilità sono infinite, poiché la tokenizzazione consente sia la proprietà frazionaria che la prova di proprietà. Dai beni tradizionali come i fondi di capitale di rischio, le obbligazioni, le materie prime e le proprietà immobiliari ai beni esotici come le squadre sportive, i cavalli da corsa, le opere d'arte e le celebrità, le aziende di tutto il mondo utilizzano la tecnologia blockchain per tokenizzare quasi tutto. Tuttavia, si possono distinguere quattro categorie principali:

* Asset: qualsiasi oggetto di valore che può essere trasformato in denaro. Si divide in due classi: personale e aziendale. Gli asset personali possono includere denaro e proprietà. Gli asset aziendali comprendono le attività presenti nel bilancio.
* Patrimonio netto (Equity): I titoli azionari (shares) possono essere tokenizzati; tuttavia, le attività rimangono sotto forma digitale di token di sicurezza memorizzati online in un portafoglio. Gli investitori possono tipicamente acquistare azioni in borsa.
* Fondi: Un fondo di investimento è un tipo di attività che gli investitori possono tokenizzare: questi token rappresentano la quota del fondo detenuta dagli investitori. Ogni investitore riceve dei token che rappresentano la sua quota del fondo.
* Servizi: Un'azienda può offrire beni o servizi come mezzo per raccogliere fondi o condurre affari. Gli investitori possono utilizzare i token per acquistare i beni o i servizi forniti dal fornitore.

I tipi di tokenizzazione della blockchain includono:

* Tokenizzazione fungibile. Si tratta di gettoni blockchain standard. Hanno valori identici, quindi possono facilmente sostituirsi l'un l'altro - si pensi a scambiare un dollaro con un altro dollaro.
* Tokenizzazione non fungibile. Si tratta di gettoni blockchain meno comuni che non hanno un valore prestabilito. Rappresentano invece la proprietà di un bene, come un'arte digitale o un immobile, che determina il valore del token.
* Tokenificazione della governance. Questi token rappresentano diritti di voto e possono essere utilizzati per votare e collaborare su un sistema blockchain.
* Tokenizzazione di utilità. Questi token sono utilizzati per dare accesso a determinati prodotti e servizi su una specifica blockchain, quindi possono essere utilizzati per completare azioni come il pagamento delle commissioni di transazione o il funzionamento di un sistema di mercato decentralizzato.

I tipi di tokenizzazione non-blockchain includono:

* Tokenizzazione del caveau. È il tipo standard di tokenizzazione per proteggere le informazioni di pagamento, in cui il token viene utilizzato per elaborare i pagamenti senza fornire numeri di carta o altri dati.
* Tokenizzazione senza caveau. È un tipo di tokenizzazione utilizzata per l'elaborazione dei pagamenti che non richiede un caveau per l'archiviazione dei token. Utilizza invece dispositivi e algoritmi crittografici per convertire i dati in token.
* Tokenizzazione con elaborazione del linguaggio naturale. Questo tipo di tokenizzazione scompone le informazioni in termini più semplici per renderle più comprensibili ai computer. Comprende la tokenizzazione di parole, sottoparole e caratteri.

Vi sono alcuni vantaggi della tokenizzazione degli asset dal punto di vista del proprietario di un bene:

* Aumento della liquidità
  + Facciamo l'esempio di una persona che richiede 50.000 dollari per un appartamento del valore di 500.000 dollari. Questo individuo potrebbe aver tokenizzato il suo appartamento in 500.000 token di sicurezza, ognuno dei quali vale lo 0,0002%. Potrebbe vendere 50.000 token, invece di vendere l'intera proprietà e perdere la sua utilità come spazio abitabile, assicurandosi così un bene più liquido.
* Prezzi equi
  + Le attività che non possono essere liquidate hanno spesso un prezzo di mercato non stabilito. In questo caso, i proprietari degli asset forniscono agli acquirenti incentivi come sconti per illiquidità, che riducono il prezzo dell'asset. La tokenizzazione degli asset aumenterebbe la liquidità di un asset, in quanto facilita la proprietà frazionata, che elimina gli sconti di illiquidità. Inoltre, la vendita di piccole frazioni di proprietà consente ai proprietari di applicare un prezzo di mercato equo.
* Riduzione dei costi di gestione
  + Se oggi si trasferisce la proprietà di un bene, è necessario l'intervento di avvocati che fungano da intermediari per gestire le pratiche burocratiche e creare fiducia tra il proprietario e l'acquirente, con conseguenti tempi e costi aggiuntivi. Se si sceglie di tokenizzare lo stesso bene e di utilizzare una piattaforma o un mercato decentralizzato, si automatizzano molte parti di questo processo, risparmiando tempo e costi.

Similmente, vi sono alcuni vantaggi della tokenizzazione degli asset dal punto di vista degli investitori:

* Aumento della liquidità
  + Considerando l'esempio precedente di una proprietà tokenizzata, è ora possibile per gli investitori al dettaglio investire piccole somme di denaro in una proprietà. Gli investitori hanno la possibilità di diversificare il loro portafoglio investendo, ad esempio, una somma di 10.000 dollari - cosa che storicamente non era possibile senza un sacco di scartoffie, che costano denaro e richiedono più tempo. Gli investitori beneficiano della maggiore liquidità degli asset grazie alla tokenizzazione.
* Periodi di blocco più brevi
  + I periodi di lock-up impediscono agli investitori di vendere i propri asset. A volte ciò è dovuto al fatto che l'asset è grande e illiquido. La tokenizzazione degli asset ha il potenziale di accorciare il periodo di lock-up, in quanto gli investitori possono vendere facilmente i loro token in un mercato liquido. In questo scenario, gli investitori non devono più aspettare anni per ottenere profitti o perdite.
* Processo trasparente
  + Poiché la tecnologia alla base della tokenizzazione degli asset, la blockchain, è immutabile, i proprietari non possono modificare la storia di un asset per farlo apparire più interessante. Ciò consente agli investitori di vedere la storia di una partecipazione e di prendere decisioni più informate.
* Identità sicura
  + Con i dati relativi alla proprietà e all'identità decentralizzata (DID) conservati sulla blockchain, la coppia di chiavi private e pubbliche dell'acquirente forma una firma digitale che garantisce che si tratti davvero di lui. Inoltre, ci sono identificatori DID decisi da organizzazioni di standard, come il w3c, che garantiscono l'accettazione in molte reti e piattaforme diverse.

Comunque, in linea di massima, possiamo evidenziare certamente:

* Maggiore accessibilità
  + L'accessibilità è anche uno dei principali vantaggi della tokenizzazione degli asset su blockchain.
  + L'adozione della tokenizzazione degli asset su blockchain consente di frammentare gli asset al minimo possibile sotto forma di token e incoraggia gli investitori a ottenere una piccola frazione di azioni. Questo apre le porte a diversi investitori e riduce il periodo e l'importo minimo di investimento.
* Assenza di intermediari e transazioni automatizzate e senza intermediari, in quanto eseguito tramite smart contract

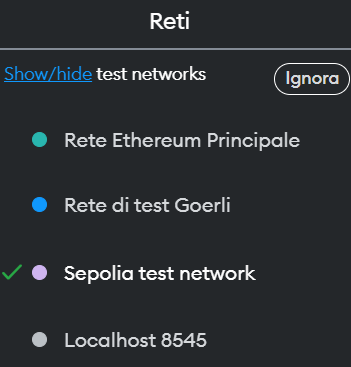
### Ambiti applicativi

Sono molti i settori che stanno abbracciando il concetto di tokenizzazione degli asset:

* Finanza
  + La tokenizzazione, una delle applicazioni della blockchain nel settore fintech, sta cambiando il panorama in diversi modi, che si tratti di prestiti a margine, strutturazione di prodotti, investimenti o pagamenti.
  + Questo concetto offre alle organizzazioni finanziarie l'opportunità di trasformare tutti gli asset in criptovalute digitali che possono essere scambiate senza soluzione di continuità. Offre ai commercianti la possibilità di evitare di memorizzare i numeri delle carte di credito nelle macchine POS e in altri sistemi. Questo, nel complesso, introduce liquidità nel mercato e riduce le violazioni della sicurezza dei dati.
  + Allo stesso modo, la tokenizzazione delle azioni fornisce agli utenti più di un token emesso per la stessa carta di credito. In altre parole, anche se si utilizza un token su un sito web online e il portale viene violato, non sarà più facile decodificare il codice e conoscere il numero effettivo della carta di credito.
  + Un esempio reale di questa tendenza emergente nelle strategie di investimento è la partnership di AlgoZ con OmiseGo.
* Immobiliare
  + Il settore immobiliare è un altro ambito di attività che sfrutta i maggiori vantaggi dello sviluppo di asset tokenizzati.
  + Il concetto di tokenizzazione immobiliare semplifica il processo di investimento. Elimina gli intermediari, rendendo più facile e conveniente l'interazione tra acquirenti e venditori. Inoltre, consente a chiunque di investire qualsiasi importo, il che si traduce in un mercato migliore per tutti.
  + Inoltre, questo concetto riduce il rischio di frode. Per questo motivo, 66 milioni di edifici saranno presto tokenizzati su Ethereum Blockchain in un accordo record.
  + Quando si parla di tokenizzazione immobiliare, ci sono diverse piattaforme che offrono servizi eccezionali in questa direzione. Alcune di esse sono Harbor, Slice e Meridio.
* Assistenza sanitaria
  + Anche il settore sanitario si sta orientando verso l'idea di adottare la tokenizzazione per risolvere alcune delle principali sfide prevalenti al giorno d'oggi.
  + La tokenizzazione sostituisce i dati sensibili dei pazienti, come informazioni sanitarie private e protette elettronicamente, con valori unici e non sensibili, riducendo così i casi di violazione dei dati. Inoltre, trasferisce il potere di creare, accedere e condividere i dati sensibili dagli intermediari come le compagnie assicurative ai pazienti e alle organizzazioni mediche. In questo modo, la tokenizzazione dei processi e delle informazioni sanitarie consente ai pazienti di convalidare l'accuratezza dei propri dati, risparmiando al contempo un'ingente somma offerta a queste terze parti.
  + Clincoin è un esempio perfetto per comprendere la portata della tokenizzazione e della token economy nel settore sanitario. Questa piattaforma basata su Blockchain, oltre a mettere in contatto utenti, fornitori e sviluppatori, premia gli utenti che si impegnano in attività salutari. Gli utenti possono poi utilizzare questi token per acquistare strumenti, prodotti e servizi digitali nel mercato decentralizzato.
* Sport
  + Un altro settore che sperimenta significativi cambiamenti positivi con l'emergere della tokenizzazione degli asset è quello dello sport.
  + La tokenizzazione degli asset sulle piattaforme blockchain decentralizza l'intero mercato, rendendo più facile per gli investitori e i fan investire nei loro giocatori e club sportivi preferiti scambiando i benefici ottenuti. Questo aiuta ulteriormente le società sportive e i giocatori a soddisfare le loro esigenze finanziarie e a operare in questo campo in modo più efficace e redditizio.
* Imprese
  + Le imprese sfruttano anche il potenziale della tokenizzazione degli asset del mondo reale nel suo monumentale passaggio alla Blockchain. Considerano questo concetto per estendere il loro approccio a nuovi mercati, valutare le prestazioni dei dipendenti, garantire una corretta allocazione delle risorse, introdurre migliori modelli di incentivazione e aggiungere trasparenza a tutti i processi interni.
  + Inoltre, le imprese introducono token diversi per i vari tipi di incarico, per offrire un'esperienza personalizzata. Stabiliscono un premio per una particolare quantità di gettoni, che aiuta a mostrare la loro importanza in termini concreti. Qualcosa che va oltre le etichette "ad alta priorità" e "urgente", che i product manager usavano in precedenza.
* Industria dell'arte
  + La blockchain può rendere l'arte più accessibile non solo agli amanti dell'arte, ma anche agli artisti, che possono ora tokenizzare le loro opere e venderle in tutto il mondo senza intermediari.
  + Uno degli esempi recenti che ha fatto notizia è stato il successo della tokenizzazione della prima opera d'arte multimilionaria. Si tratta di un dipinto di Andy Warhol chiamato "14 Small Electric Chairs (1980)". Lo scopo principale dell'asta beta era quello di testare il processo d'asta olandese e in generale verificare il funzionamento della tokenizzazione delle opere d'arte e della tecnologia blockchain.

### Come creare un token

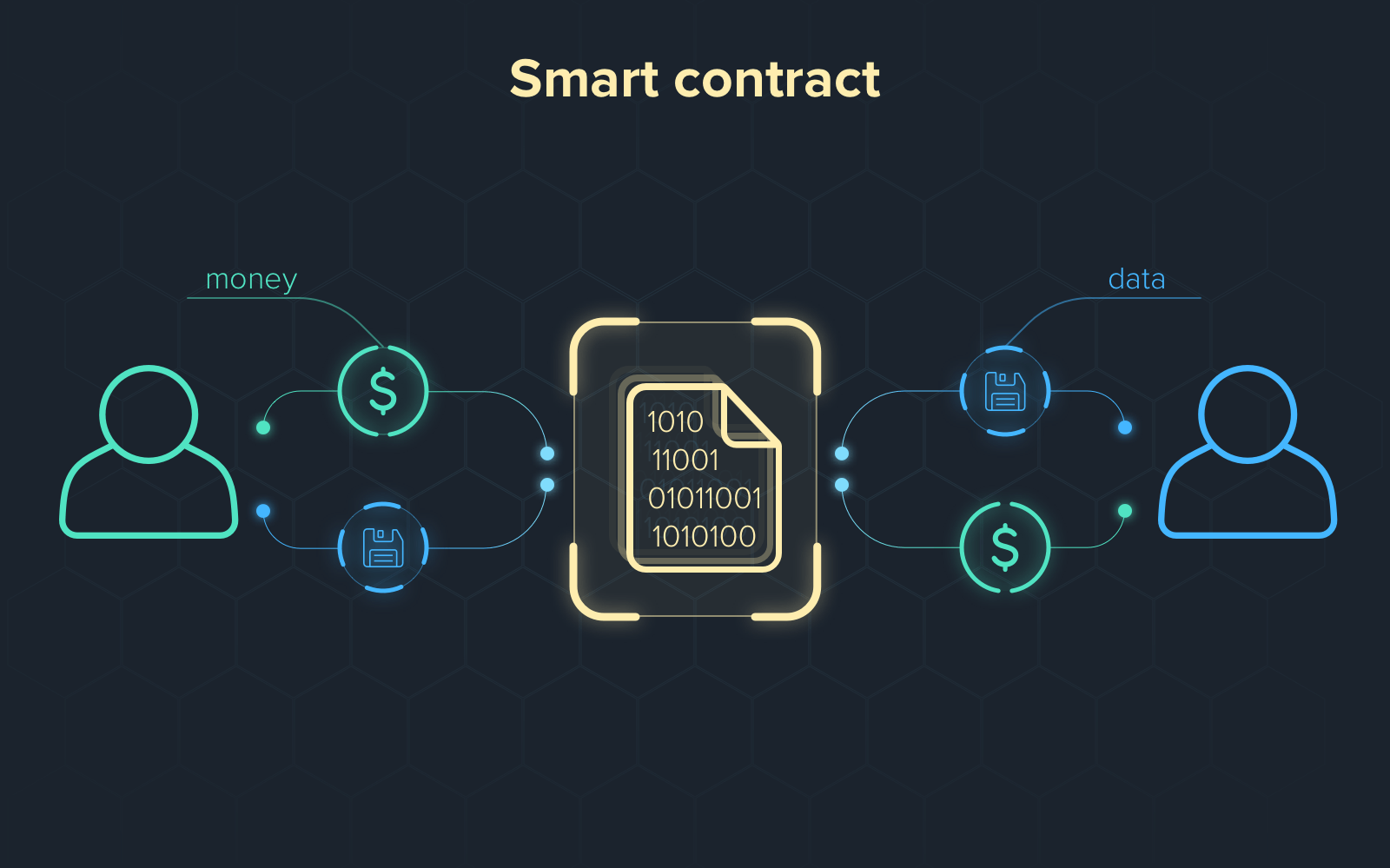
* Decidere quali problemi aziendali risolverà il token e a quale pubblico sarà rivolta
  + Molte persone che si avvicinano al settore delle criptovalute non capiscono cosa stia succedendo nella tecnologia blockchain e vogliono semplicemente guadagnare vendendo token.
  + Ad esempio, se parliamo di ICO, la maggior parte di esse è stata creata per fare soldi dal nulla. I loro creatori non sanno quanti utenti utilizzeranno i loro progetti o se ci sarà una domanda per i token emessi durante le ICO. Di conseguenza, molti team falliscono dopo il lancio a causa della mancanza di domanda per i loro servizi o prodotti.
  + Per questo motivo, il primo passo per la creazione di un token crittografico è decidere quali problemi aziendali risolverà il token, perché ne ha bisogno e se ne ha bisogno. Questo punto è importante per definire ulteriormente le caratteristiche del token e quindi per preparare un piano di progetto.
* Usare un wallet come MetaMask, CoinBase o similari, al fine di crearsi un account, associarsi una frase segreta e avere un posto dove depositare le valute per fare prove



* Usare i cosiddetti *faucet*, cioè dei siti che danno ricompense sulle cosiddette testnet (reti di test attivabili nelle impostazioni, come le seguenti:
* Creare uno smart contract di esempio, che definisca il token.
  + Un esempio può essere anche qui:
    - <https://levelup.gitconnected.com/how-to-create-a-cryptocurrency-token-15a898e2bb8d>
  + In questo definire il numero di token, decimali, il nome e l’abbreviazione

## Smart contract

Gli smart contract sono programmi che automatizzano le azioni richieste in un accordo o contratto, considerate tracciate e irreversibili. Essi sono programmi informatici auto-eseguibili che vengono eseguiti su una blockchain. In pratica, sono contratti digitali che automatizzano ed eseguono le clausole contrattuali in modo sicuro, trasparente e immutabile, senza la necessità di intermediari.



Riferimento: <https://www.arlawpractice.com/gli-smart-contract-cosa-sono-e-come-funzionano/>

* Possono essere considerati programmi event-driven che girano su un libro mastro decentralizzato, distribuito, condiviso e replicato che possono prendere in custodia e istruire il trasferimento di beni su quel libro mastro.
* Poiché i contratti intelligenti eseguono accordi, possono essere utilizzati per molti scopi diversi. Uno degli usi più semplici è quello di garantire che le transazioni tra due parti avvengano, come l'acquisto e la consegna di merci. Ad esempio, un produttore che ha bisogno di materie prime può impostare i pagamenti utilizzando gli smart contract e il fornitore può impostare le spedizioni. Poi, a seconda dell'accordo tra le due aziende, i fondi potrebbero essere trasferiti automaticamente al fornitore al momento della spedizione o della consegna.

L'esecuzione della transazione non prevede l'intervento di alcun intermediario. I partecipanti devono

firmare crittograficamente la loro partecipazione.

- I contratti intelligenti dispongono di interfacce di input che ricevono i dati in ingresso.

- I dati vengono interpretati e convalidati secondo le regole programmate.

- Le firme delle parti coinvolte nella transazione vengono verificate.

Nell'insieme degli smart contract di una blockchain, uno smart contract può agire in modo isolato dagli altri o interagire con essi per completare i compiti affidati. In questo modo, è possibile progettare suite di smart contract per scopi specifici.

Così, uno smart contract può concentrarsi sulla ricezione di dati dall'esterno, mentre un altro smart contract può concentrarsi sull'elaborazione di regole aziendali. Infine, un altro smart contract può occuparsi di dare persistenza al risultato (gli smart contract elaborano le loro istruzioni e alla fine producono un risultato da memorizzare nella blockchain).

* Gli scambi effettuati tramite smart contract sono definite DEX (decentralized exchanges) che consentono agli utenti di negoziare criptovalute e altri asset digitali senza la necessità di un intermediario centralizzato, come una borsa tradizionale o un broker. I DEX sono stati creati per eliminare la necessità di un'autorità che supervisionasse e autorizzasse le transazioni. A differenza delle borse centralizzate, i DEX non custodiscono i fondi degli utenti, che sono responsabili della loro perdita in caso di errore.
  + In un DEX, i contratti intelligenti vengono utilizzati per eseguire automaticamente le transazioni tra acquirenti e venditori. I contratti intelligenti fungono da "intermediari" e assicurano che le transazioni siano eseguite in modo sicuro e trasparente. Questi contratti sono auto-esecutivi e auto-applicativi, il che significa che eseguiranno automaticamente la compravendita non appena le condizioni stabilite nel contratto saranno soddisfatte.
  + I DEX possono essere progettati in modi diversi, ma in genere prevedono tutti l'uso di contratti intelligenti. Ad esempio, alcuni DEX utilizzano un modello di market maker automatizzato (AMM), in cui il prezzo di un'attività è determinato da un algoritmo che bilancia la domanda e l'offerta dell'attività. Altri utilizzano un modello tradizionale di portafoglio ordini, in cui acquirenti e venditori possono piazzare ordini limite o di mercato.
  + Ci sono tre tipi principali di DEX:
    - *Order books DEX*, che raccolgono le registrazioni di tutti gli ordini aperti di acquisto e vendita di asset per coppie di asset specifiche. Gli ordini di acquisto indicano che un trader è disposto ad acquistare o fare un'offerta per un asset a un prezzo specifico, mentre gli ordini di vendita indicano che un trader è pronto a vendere o chiedere un determinato prezzo per l'asset in questione. Lo spread tra questi prezzi determina la profondità del portafoglio ordini e il prezzo di mercato della borsa.
      * I DEX con order book sono di due tipi: order book on-chain e order book off-chain. I DEX che utilizzano gli order book spesso conservano le informazioni sugli ordini aperti sulla catena, mentre i fondi degli utenti rimangono nei loro portafogli. Queste borse possono consentire ai trader di fare leva sulle loro posizioni utilizzando fondi presi in prestito da prestatori sulla loro piattaforma. Il trading con leva aumenta il potenziale di guadagno di un'operazione, ma aumenta anche il rischio di liquidazione, poiché aumenta la dimensione della posizione con i fondi presi in prestito, che devono essere rimborsati anche se i trader perdono la loro scommessa.
      * Tuttavia, le piattaforme DEX che tengono i loro order book fuori dalla blockchain regolano le transazioni solo sulla blockchain per portare ai trader i vantaggi delle borse centralizzate. L'uso di libri degli ordini fuori dalla catena aiuta le borse a ridurre i costi e ad aumentare la velocità per garantire che le transazioni siano eseguite ai prezzi desiderati dagli utenti.
      * È importante sottolineare che i DEX con order book spesso soffrono di problemi di liquidità. Dato che sono essenzialmente in concorrenza con le borse centralizzate e che devono sostenere commissioni aggiuntive rispetto a quelle che si pagano per le transazioni on-chain, i trader di solito si attengono alle piattaforme centralizzate. Mentre i DEX con order book off-chain riducono questi costi, i rischi legati agli smart contract sorgono a causa della necessità di depositare fondi in essi.
    - *Automated Market Makers (AMM)*, che risolvono il problema della liquidità e si affidano a servizi basati sulla blockchain che forniscono informazioni dalle borse e da altre piattaforme per stabilire il prezzo degli asset scambiati, chiamati oracoli della blockchain. Invece di far coincidere gli ordini di acquisto con quelli di vendita, gli smart contract di queste borse decentralizzate utilizzano pool di asset prefinanziati noti come pool di liquidità.
      * I pool sono finanziati da altri utenti che hanno diritto alle commissioni di transazione che il protocollo addebita per l'esecuzione degli scambi su quella coppia. Questi fornitori di liquidità devono depositare un valore equivalente di ogni asset nella coppia di trading per guadagnare interessi sulle loro criptovalute, un processo noto come liquidity mining. Se tentano di depositare una quantità maggiore di un asset rispetto all'altro, lo smart contract alla base del pool invalida la transazione.
      * L'uso dei pool di liquidità consente ai trader di eseguire ordini o di guadagnare interessi in un modo privo di autorizzazioni e di fiducia. Queste borse sono spesso classificate in base alla quantità di fondi bloccati nei loro smart contract, chiamata valore totale bloccato (TVL), poiché il modello AMM ha un lato negativo quando non c'è abbastanza liquidità: lo slippage.
      * Lo slippage si verifica quando la mancanza di liquidità sulla piattaforma fa sì che l'acquirente paghi prezzi superiori a quelli di mercato per il suo ordine, con ordini più grandi che subiscono uno slippage maggiore. La mancanza di liquidità può dissuadere i trader più facoltosi dall'utilizzare queste piattaforme, in quanto gli ordini di grandi dimensioni rischiano di subire uno slippage in assenza di liquidità profonda.
      * I fornitori di liquidità devono inoltre affrontare vari rischi, tra cui la perdita impermanente, che è il risultato diretto del deposito di due asset per una specifica coppia di trading. Quando uno di questi asset è più volatile dell'altro, gli scambi in borsa possono ridurre la quantità di un asset nel pool di liquidità.
      * Se il prezzo dell'asset altamente volatile aumenta mentre la quantità di liquidità detenuta dai fornitori di liquidità diminuisce, questi ultimi subiscono una perdita impermanente. La perdita è impermanente perché il prezzo dell'attività può ancora risalire e gli scambi in borsa possono bilanciare il rapporto di coppia. Il rapporto di coppia descrive la proporzione di ciascun asset detenuto nel pool di liquidità. Inoltre, le commissioni incassate dal trading possono compensare la perdita nel tempo.
    - *DEX Aggregators*, che utilizzano diversi protocolli e meccanismi per risolvere i problemi associati alla liquidità. Queste piattaforme aggregano essenzialmente la liquidità di diversi DEX per minimizzare lo slippage sugli ordini di grandi dimensioni, ottimizzare le commissioni di swap e i prezzi dei token e offrire ai trader il miglior prezzo possibile nel minor tempo possibile.
      * Proteggere gli utenti dall'effetto prezzo e diminuire la probabilità di transazioni non andate a buon fine sono altri due obiettivi significativi degli aggregatori DEX. Alcuni aggregatori DEX utilizzano anche la liquidità delle piattaforme centralizzate per offrire agli utenti un'esperienza migliore, pur rimanendo non depositari grazie all'integrazione con specifiche borse centralizzate.

A livello di vantaggi:

* Decentralizzazione: I DEX operano su una rete decentralizzata e non si affidano a intermediari, come le autorità centrali, per eseguire le transazioni. Questo riduce il rischio di censura, manipolazione e furto.
* Privacy: Gli utenti non devono rivelare la propria identità o le proprie informazioni personali per utilizzare i DEX. Questo garantisce una maggiore privacy e anonimato.
* Sicurezza: I DEX sono più sicuri delle borse centralizzate poiché utilizzano contratti intelligenti e la tecnologia blockchain per eseguire le transazioni. Questo rende difficile per gli hacker manipolare il sistema e rubare i fondi.
* Accesso a una gamma più ampia di token: I DEX offrono l'accesso a una gamma più ampia di token, compresi quelli che non sono disponibili nelle borse centralizzate.
* Commissioni più basse: I DEX hanno spesso commissioni più basse rispetto alle borse centralizzate, in quanto non devono pagare per costose infrastrutture e conformità normativa.

A livello di svantaggi:

* Problemi di liquidità: I DEX soffrono spesso di problemi di liquidità, che possono causare slittamenti e costi di transazione più elevati per gli ordini di grandi dimensioni.
* Complessità: I DEX possono essere più complessi da usare rispetto alle borse centralizzate, il che può dissuadere alcuni utenti dall'utilizzarli.
* Mancanza di controllo normativo: Poiché i DEX operano su una rete decentralizzata, non hanno lo stesso livello di supervisione normativa delle borse centralizzate. Ciò può rendere difficile la risoluzione delle controversie e l'applicazione delle leggi a tutela dei consumatori.
* Vulnerabilità al front-running: I DEX sono vulnerabili agli attacchi di front-running, in cui i trader utilizzano algoritmi avanzati per vedere e agire sugli ordini di altri trader prima che vengano eseguiti.
* Perdita impermanente: I fornitori di liquidità sui DEX possono subire una perdita impermanente, che è il risultato diretto del deposito di due asset per una specifica coppia di trading. Quando uno di questi asset è più volatile dell'altro, gli scambi in borsa possono ridurre la quantità di un asset nel pool di liquidità, con conseguente perdita per il fornitore di liquidità.

### Come funzionano

Il funzionamento di uno smart contract è simile a quello di altri trasferimenti su blockchain. Questi sono i passi necessari:

1. Un utente avvia una transazione dal proprio portafoglio blockchain;
2. la transazione arriva al database distribuito, dove viene confermata l'identità del portafoglio dell'utente;
3. la transazione, che può essere un trasferimento di fondi e comprende il codice che definisce il tipo di transazione da eseguire, viene approvata;
4. le transazioni vengono aggiunte come blocco all'interno della blockchain;
5. qualsiasi modifica dello stato del contratto segue lo stesso processo per essere aggiornata.

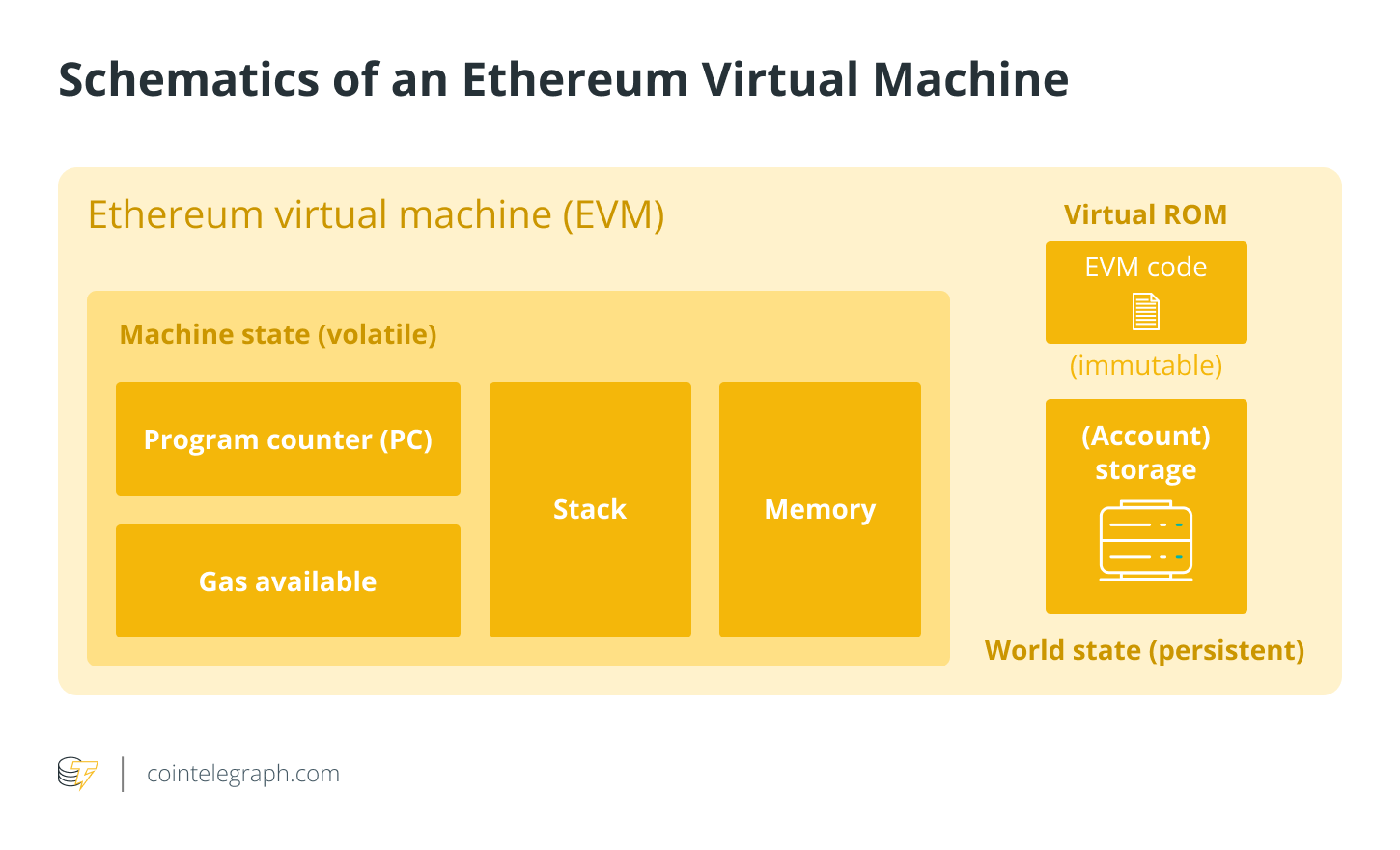
L’approvazione degli smart contract è definita trustless, dunque non si ha bisogno di una società intermediata e la gestione dei fondi è in mano ai validatori per le transazioni, agli staker per il Proof of Stake e i miner per il Proof of Work.

Gli smart contracts sono Turing-complete, pertanto possono potenzialmente essere eseguiti per sempre, bloccando ogni singolo nodo sulla blockchain.

### Dove vengono usati

Tra le piattaforme più vastamente utilizzate per sviluppare ed eseguire degli smart contract abbiamo:

* *Ethereum*: i contratti intelligenti sono scritti in un linguaggio di programmazione chiamato Solidity e vengono eseguiti dalla macchina virtuale di Ethereum (Ethereum Virtual Machine/EVM), Ethereum è considerata la piattaforma più popolare e la sua macchina virtuale di Ethereum è un motore di calcolo responsabile dell'implementazione, dell'esecuzione dei contratti smart e di calcolare lo stato di ogni nuovo blocco aggiunto alla blockchain di Ethereum.



Riferimento: <https://cointelegraph.com/news/what-is-an-ethereum-virtual-machine-evm-and-how-does-it-work>

* + La Ethereum Virtual Machine (EVM) è progettata come ambiente di runtime per i contratti intelligenti in Ethereum. È isolata dalle altre parti del sistema; ciò significa che qualsiasi operazione sulla EVM non dovrebbe influire in alcun modo sui dati o sui programmi, indipendentemente dal numero di volte in cui si chiama una particolare funzione.
  + La macchina è stata realizzata per essere in grado di eseguire qualsiasi tipo di contratto crittografico che possa essere costruito sulla blockchain di Ethereum. Per farlo utilizza un linguaggio di programmazione chiamato Solidity, che viene compilato nell'EVM per l'esecuzione. In questo modo, verranno creati degli smart contract e programmi che eseguono automaticamente solo quando certe condizioni si verificano.
  + Essa fornisce un ambiente Turing-complete per l'esecuzione di script e contratti intelligenti. Ciò significa che tutto ciò che può essere implementato con un computer può essere eseguito su EVM. Infatti, ogni nodo della rete di Ethereum deve accordarsi con quello successivo per eseguire le stesse istruzioni. Di fatto è un singleton e ognuno dei nodi esegue una copia locale della EVM. Tutte le operazioni sono eseguite su un’area dati virtuale denominata “stack”, formata da 1024 words di 256 bit.
  + Essa ha due parti principali:
    - EVM (la parte che esegue il codice sorgente di Solidity): La EVM è scritta in C++ e utilizza LLVM come compilatore. È una macchina virtuale completa con tutte le caratteristiche che si possono desiderare in una macchina virtuale per smart contract di uso generale, come il supporto di più linguaggi di programmazione, funzioni di sicurezza, ambienti di runtime e altro ancora. Consente inoltre di scrivere bytecode EVM personalizzati.
    - Zii (Uncles): Si tratta di piccoli pezzi di smart contract o di dati memorizzati sulla blockchain. È una funzione utile perché consente di memorizzare metadati sul programma.
  + La criptovaluta nativa della piattaforma Ethereum è ETH, definita anche come Ether. Questa valuta è l’oggetto di scambi degli smart contracts. Di fatto, ne vengono create 5 ogni 12 secondi. Il consenso si raggiunge tramite proof-of-stake. Possiamo inoltre distinguere ETC (Ethereum Classic), hard fork di Ethereum (ETH), che permette su di essa l’esecuzione degli smart contract. La politica viene modificata, riducendo la ricompensa del blocco del 20% al 5 milionesimo numero di blocco e del 20% ogni 5 milionesimi.
  + All’interno di questa rete si parla di *gas* come il costo aggiuntivo richiesto per eseguire uno smart contract o una transazione sulla rete blockchain. È ciò che permette anche ai minatori (prima) e ai validatori (ora) di trarre profitto e fornisce un incentivo per svolgere il lavoro necessario a proporre il prossimo blocco di transazioni per la blockchain. Due fattori determinano la quantità di gas richiesta da una transazioni:
    - La sua complessità
      * Questo si determina tramite la presenza degli *opcode*, presenti nel bytecode (intermedio tra linguaggio macchina e linguaggio di programmazione) di EVM, che determina la complessità di ciascuna operazione (es. STOP, ADD, MUL, SUB, etc.). Esiste una lista completa dei vari opcodes con un consumo di gas ad essi associato.
    - Il carico corrente sulla rete Ethereum
      * La formula per il calcolo del gas è:

.

Il prezzo della tariffa base è determinato dalla congestione della rete di Ethereum. La mancia è una tassa prioritaria e viene impostata automaticamente dalla maggior parte dei portafogli per accelerare il completamento della transazione, quindi non è molto importante per il calcolo del gas.

* + - * La commissione di base per il blocco corrente è calcolata in base ai blocchi precedenti. Quando un nuovo blocco viene aggiunto alla blockchain, c'è una quantità prestabilita di gas, chiamata gas incluso, che può contenere (somma di tutte le commissioni del gas dalle transazioni nel blocco).
  + La presenza della EVM permette l’esecuzione di codice non sicuro senza perdere dati, interagendo anche con contratti complicati e con un calcolo deterministico. Grazie al fatto che ogni nodo deve raggiungere consenso ad ogni momento, si ha che il sistema risulti essere più sicuro e robusto contro i fallimenti. Inoltre può costruire contratti stateful (cioè, validi e memorizzabili su un supporto)
  + La transazione dovrà sempre indicare:
    - GAS PRICE: prezzo che l’autore di una transazione può pagare per unità di gas ed incide sulla rapidità con cui la transazione verrà incluso in un blocco aggiunto alla blockchain. Se si ha un prezzo alto, si avranno commissioni maggiori per i nodi che aggiungeranno il blocco alla blockchain (miner); questi tenderanno a massimizzare il loro guadagno per blocco.
    - GAS LIMIT: quantità massima di unità di gas che si è disposti a spendere per l’esecuzione della transazione attuale. Se la transazione può consumare più risorse di quelle assegnate, l’esecuzione si blocca e la transazione fallisce non impegnando altre risorse, mentre se inferiore, la restante parte verrà rimborsata in Ether all’autore della transazione.
* *Hyperledger*: è un sistema open source sviluppato dalla Linux Foundation e non è una blockchain, ma una piattaforma flessibile su cui è possibile sviluppare contratti intelligenti.
* *Polkadot*: è un'alternativa alla blockchain ed è famosa per la sua capacità di ospitare parachain, cioè catene all'interno di catene, consentendo un numero maggiore di transazioni rispetto al normale.
* *Solana*: gli smart contract Solana possono essere creati utilizzando diversi linguaggi di programmazione. Mentre il linguaggio nativo per i contatti intelligenti di Solana è Rust, il protocollo supporta anche lo sviluppo di contratti intelligenti in C++ e Solidity, oltre che in C++ e Solidity, oltre al supporto di altri linguaggi attraverso client JSON RPC API SDK di terze parti.
* *Cosmos*: Cosmos è un ecosistema in espansione di blockchain indipendenti e interconnesse collegate attraverso il protocollo Inter-Blockchain Communication. Gli sviluppatori possono scegliere di costruire blockchain autonome e specifiche per le applicazioni che possono facilmente interconnettersi. Il protocollo standard per la comunicazione inter blockchain, l'IBC, consente alle blockchain dell'ecosistema di connettersi in modo da poter trasferire token e altri dati tra le blockchain. Cosmos attualmente ha tre diversi SDK che consentono agli sviluppatori di scrivere contratti intelligenti in Javascript, Rust o Solidity.
* *Stellar*: Stellar è stata fondata nel 2014, il che la rende una delle più antiche piattaforme di contratti intelligenti. È mantenuta dalla Stellar Development Foundation ed è stata ripetutamente proclamata come una delle più interessanti startup blockchain in circolazione.

### Tipologie

* Smart Legal Contracts (Contratti legali intelligenti)
  + Questi contratti sono legalmente applicabili e richiedono alle parti di soddisfare i loro obblighi contrattuali. Le parti possono incorrere in severe azioni legali in caso di inadempienza.
  + Per creare alcuni contratti legali intelligenti, le parti coinvolte lavorano sul codice del contratto intelligente - o lo fanno i loro sviluppatori di software - finché non si accordano sui termini e sulle condizioni dell'accordo. Altri contratti blockchain, come quelli dei siti di scommesse, sono creati da terzi. In entrambi i casi, le parti che stipulano un accordo non hanno bisogno di incontrarsi di persona o di conoscere l'identità dell'altro. Ciascuna di esse può apporre una firma digitale e lo status giuridico del contratto viene ufficializzato.
* Esempio reale:
  + Con l'avvento dei contratti intelligenti, il regno del diritto contrattuale si sta spostando in forma digitale. Home Depot utilizza contratti legali intelligenti con i fornitori. Il direttore delle operazioni finanziarie di Home Depot, Brian Quartel, spiega in un caso di studio IBM che stanno essenzialmente creando visibilità tra loro e i loro fornitori su ciò che è stato spedito e ricevuto.
  + L'attuale quadro giuridico per i contratti intelligenti varia nei sistemi giudiziari di varie regioni e nazioni. Esperti legali e associazioni stanno lavorando per definire uno smart contract legalmente applicabile e i processi si stanno evolvendo man mano che diventano più comuni. In California, ad esempio, è già possibile sposarsi con una licenza di matrimonio per smart contract.
* Organizzazioni autonome decentralizzate (DAO)
  + Per una DAO, la spina dorsale è il suo contratto intelligente. Il contratto è vincolato a regole specifiche che sono codificate nei contratti della blockchain e che si fondono con i meccanismi di governance. Ha diversi casi d'uso che vanno dal semplice al complesso, a seconda del numero di parti interessate.
  + Le DAO sono open-source e sono caratterizzate da trasparenza e, in teoria, sono incorruttibili. Inoltre, qualsiasi azione intrapresa dai membri della comunità viene sostituita da un codice auto-applicativo.
  + Possono essere autonome e autosufficienti utilizzando il codice dei contratti intelligenti concordato da tutti i partecipanti che hanno fondato la DAO, e il codice e la struttura aziendale possono evolvere utilizzando qualsiasi sistema di voto stabilito dalla DAO.
  + Essendo privo di fiducia, il codice persisterà con o senza gestione. Il cambio di leadership non influenza lo scopo, la visione o la funzione della DAO. E come tutti i contratti intelligenti, i DAO sono open source. Sono visibili a tutti i membri e non membri del DAO; i bug possono essere corretti e i suggerimenti possono essere proposti al DAO da chiunque.
* Esempio reale:
  + Nel febbraio 2022 è nata una collaborazione a tre tra Molecule, un'azienda di tecnologia decentralizzata, Apollo Health Ventures, un fondo di venture capital focalizzato sulla ricerca sulla longevità, e VitaDAO, un DAO focalizzato sul finanziamento della ricerca sulla longevità.
  + VitaDAO crea opportunità di finanziamento per gli scienziati biotecnologici senza richiedere sovvenzioni o registrare brevetti. A ogni progetto che VitaDAO prende in carico viene assegnato un IP-NFT, ovvero un gettone di proprietà intellettuale non fungibile. In questo modo, i membri del DAO gestiscono le proposte di ricerca e i loro progressi, assegnano i fondi ai ricercatori scelti e trovano persino i pazienti per la ricerca.
  + Oltre a eliminare la gerarchia aziendale dalle strutture di business, una DAO completamente autonoma gestirà transazioni come la revisione tra pari dei membri del team e l'assegnazione di token per i compiti portati a termine.
* Contratti logici applicativi (ALC)
  + Un altro tipo di smart contract in Blockchain è rappresentato dagli Application Logic Contracts (ALC), che consentono ai dispositivi di funzionare in modo sicuro e autonomo. Inoltre, gli ALC garantiscono una maggiore automazione, transazioni più economiche e scalabilità.
  + Questi contratti contengono un codice basato su un'applicazione, che di solito rimane sincronizzato con altri contratti blockchain. Consentono la comunicazione tra diversi dispositivi, come la fusione dell'Internet delle cose (IoT) con la tecnologia blockchain.
* Esempio reale
  + Beam Technologies, una startup con sede a Columbus, Ohio, ha lanciato uno spazzolino intelligente. Lo spazzolino è coordinato con la compagnia assicurativa dentale recentemente lanciata, che utilizza sensori nello spazzolino per raccogliere dati sull'igiene dentale dell'utente. Lo spazzolino "dialoga" con Beam Dental e influisce sulle tariffe del premio dentale dell'utente: più a lungo si usa lo spazzolino e più volte lo si usa ogni giorno, più il premio si riduce.
  + La chiave per gli ALC nell'ambito dell'Internet degli oggetti è l'esecuzione automatizzata del trasferimento dei dati, che attiva risposte diverse. Utilizzando il codice basato sulle applicazioni e la blockchain come spina dorsale per il trasferimento e l'archiviazione sicuri dei dati, gli sviluppatori possono trovare innumerevoli ruoli inventivi che gli ALC possono svolgere.

### Pro e contro

Alcuni dei vantaggi più degni di nota dei contratti intelligenti sono i seguenti:

* *Validità giuridica immediata*

In merito ai contrati intelligenti, questi pongono un meccanismo di vincolatività nella tecnologia blockchain e smart contract che impedisce dall’inizio l’inadempimento; infatti, per un nodo è tecnicamente impossibile violare volontariamente le condizioni prestabilite e ciò pone in secondo piano conseguenze legate all’inadempimento.

* *Velocità ed efficienza*

Grazie all'elevato grado di automazione e all'autoesecuzione dei termini concordati, i contratti intelligenti semplificano l'intero ciclo di vita dell'implementazione del contratto, contribuendo a un'esecuzione rapida, continua ed efficiente. Alcuni vantaggi facilmente raggiungibili che i contratti intelligenti consentono di ottenere: pagamenti automatizzati, richieste di risarcimento assicurativo, catene di fornitura trasparenti ed efficienti, efficienza aziendale, catene di fornitura trasparenti ed efficienti, una governance aziendale efficiente o lo snellimento della gestione dei dati per gli studi clinici.

* *Trasparenza*

I contratti intelligenti contribuiscono a garantire una maggiore trasparenza e allo stesso tempo a ridurre le possibilità di corruzione, dal momento che qualsiasi modifiche apportate al contratto richiedono il consenso di tutte le parti coinvolte o almeno possono essere rintracciate facilmente. La possibilità di manipolazione o di inadempimento da parte di un singolo individuo è altamente improbabile.

* *Sicurezza*

Grazie all'uso della crittografia dei dati, i contratti intelligenti sono a prova di manomissione e rappresentano un'alternativa altamente sicura ai contratti cartacei. I contratti intelligenti sono pezzi di codice che possono essere prontamente riutilizzati per operazioni simili con modifiche minime in base ai requisiti

* *Eliminazione degli intermediari e convenienza economica*

Eliminando la necessità di terze parti o intermediari per l'esecuzione, gli smart contract eliminano il rischio di manipolazione. I risparmi sui costi derivano dalla rimozione dei livelli di intermediazione nelle relazioni e nelle transazioni peer-to-peer. L'esecuzione automatica dei contratti intelligenti elimina potenzialmente la necessità di un'applicazione istituzionale e presenta un'alternativa più economica ed efficace per la garanzia ex-ante della performance. L'utilizzo degli smart contract comporta l'eliminazione degli errori dovuti alla compilazione manuale di numerosi moduli.

Possiamo tuttavia citare una serie di svantaggi:

* Il primo riguarda l'incapacità degli smart contract di valutare gli eventi del mondo reale. Questo non deve sorprendere, poiché le blockchain sono generalmente ambienti indipendenti e separati. La separazione è un meccanismo che garantisce la sicurezza della rete sulla base dell'algoritmo di consenso.
  + Di conseguenza, i dati che risiedono nei database, dalle informazioni sui dipendenti a dati qualsiasi relativi al mondo esterno, sono dati al di fuori della blockchain considerati potenzialmente pericolosi per la rete stessa.
* La seconda limitazione fa riferimento alla dimensioni massime dei contratti per gli smart contract. La limitazione è definita dal protocollo EIP-170 che previene gli attacchi DOS (Denial of Service) attraverso l'esecuzione di contratti infiniti per congestionare la rete. Gli sviluppatori sono tenuti a includere funzionalità che non superino il limite massimo di 24 KB.

### Considerazioni legali e casi d’uso

* Il Parlamento italiano ha approvato la legge n. 12/2019, che definisce la tecnologia distributed ledger e convalida gli smart contract con forma scritta. La legge indica che un documento informatico registrato tramite DLT ha gli effetti legali della validazione temporale elettronica. Inoltre, stabilisce che gli smart contract sono programmi informatici che operano su ledger distribuiti e la loro esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti, dando completa equivalenza tra contratti cartacei e documenti digitali
* La Commissione giuridica del Regno Unito raccomanda che il quadro giuridico in Inghilterra e Galles supporti l'uso dei contratti legali intelligenti. Definisce tre categorie di contratti legali intelligenti, ma è necessario affrontare questioni relative alla formazione del contratto, all'interpretazione, alla protezione dei consumatori, ai rimedi e alla giurisdizione. Secondo il diritto inglese, i requisiti per un contratto legalmente vincolante possono essere soddisfatti da uno smart contract. Tuttavia, l'aggiunta di codice nel mix interpretativo può dare origine a difficoltà interpretative, richiedendo a una persona ragionevole con conoscenza e comprensione del codice di capire il significato del contratto.

Alcuni casi d’uso includono:

* Le *DAO (Decentralized Autonomous Organizations)* sono un tipo di struttura di governance organizzativa che consiste in comunità native di Internet che lavorano con l'infrastruttura digitale e che si concentrano sulla condivisione di un'infrastruttura digitale e si concentrano su una missione condivisa e su un protocollo blockchain. Esse sono gestite e possedute dai contributori (membri) della comunità, e operano in modo fluido dal basso verso l'alto con una struttura piatta, ma comunque strutturata.
  + Nel contesto delle DAO, gli smart contract sono utilizzati per rappresentare beni e capitali sotto forma di token, che possono essere utilizzati per esercitare il potere di voto, governare un protocollo, allocare fondi e incentivare la partecipazione alla rete. Ad esempio, quando un membro della DAO vuole votare su una proposta, può utilizzare i propri token per esprimere il proprio voto attraverso uno smart contract. Se la proposta viene approvata con il numero di voti richiesto, lo smart contract eseguirà automaticamente le azioni specificate nella proposta, come l'assegnazione di fondi a un progetto specifico o l'aggiornamento del codice del protocollo.
* *DeFi* (*Decentralized Finance)* è un ecosistema in rapida crescita di applicazioni finanziarie costruite sulla base della tecnologia blockchain. Le applicazioni DeFi sono progettate per fornire servizi finanziari in modo decentralizzato, aperto e senza permessi, consentendo a chiunque abbia una connessione a Internet e un portafoglio di criptovalute di partecipare al sistema finanziario globale senza la necessità di intermediari tradizionali come banche o istituzioni finanziarie.
  + Gli smart contract sono utilizzati per creare protocolli finanziari accessibili e utilizzabili da chiunque abbia una connessione a Internet, senza bisogno di intermediari come banche o istituzioni finanziarie. Questi protocolli possono essere utilizzati per un'ampia gamma di attività finanziarie, come prestiti, mutui, scambi e assicurazioni.
    - Ad esempio, in un protocollo di prestito DeFi, gli smart contract sono utilizzati per automatizzare il processo di prestito e di erogazione. I mutuatari possono presentare garanzie sotto forma di criptovalute, che vengono tenute in deposito dallo smart contract. Il contratto emette quindi automaticamente un prestito nella valuta desiderata, con i termini del prestito e il tasso di interesse specificati nel contratto stesso. Il mutuatario deve rimborsare il prestito più gli interessi entro una certa data, altrimenti la garanzia viene incamerata dal mutuante.
    - Allo stesso modo, in un protocollo di trading DeFi, gli smart contract sono utilizzati per eseguire le transazioni tra le parti. Gli acquirenti e i venditori possono inviare i loro ordini allo smart contract, che li confronta in base ai criteri specificati. Lo smart contract esegue quindi la compravendita, trasferendo gli asset tra le parti e aggiornando i rispettivi saldi dei conti.

### Possibili problemi

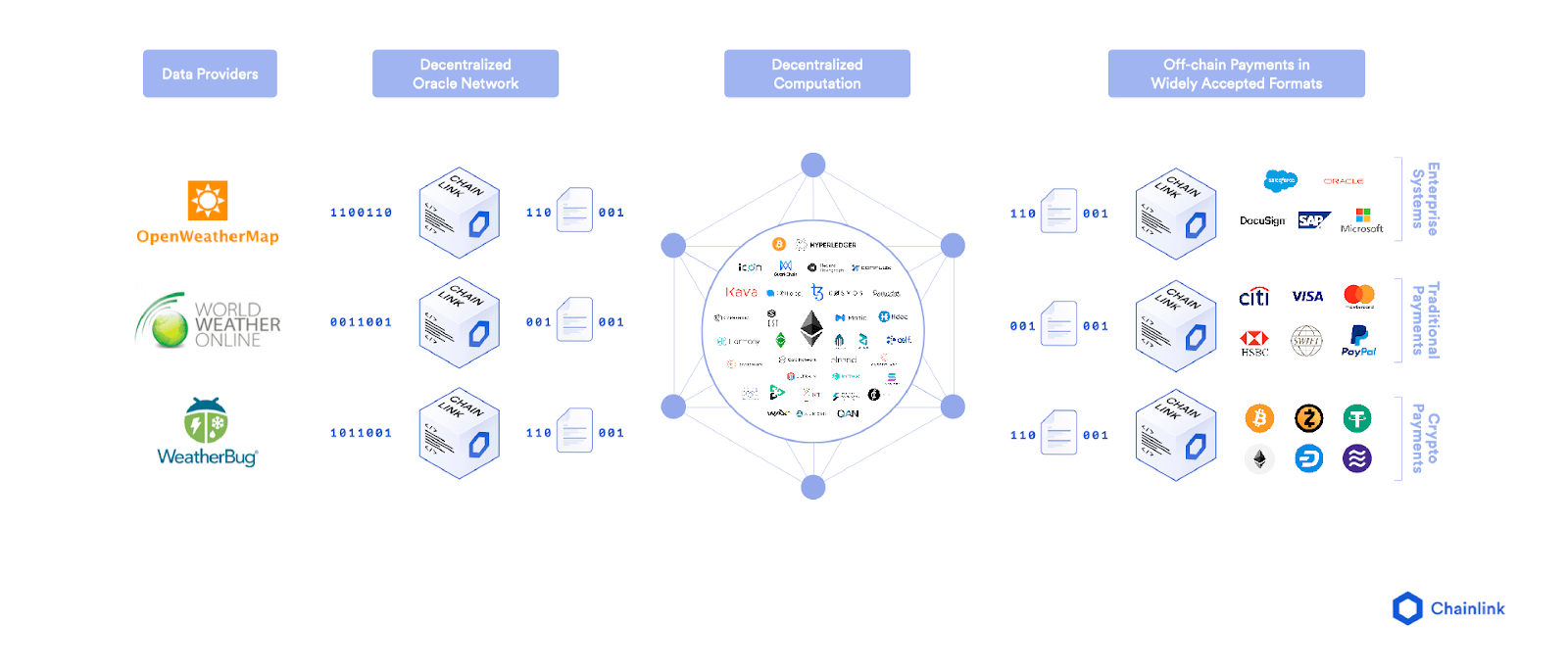
Per loro natura, gli smart contract sono deterministici e tutti i nodi all’interno della sua rete devono raggiungere tutti il consenso. I contratti smart minimizzano efficacemente il rischio di controparte e forniscono trasparenza, ma presentano ancora diversi limiti alla loro capacità.

* La crescente necessità di dati esterni che confluiscono nelle blockchain e, per estensione, negli smart contract ha portato a dibattiti e innovazioni intorno agli oracoli (oracles), che sono flussi di dati provenienti da sistemi esterni che alimentano le blockchain con informazioni vitali che gli smart contract possono avere bisogno di eseguire in condizioni specifiche. La crescente necessità di oracoli rappresenta la continua espansione dei sistemi blockchain in casi d'uso pratici e reali, dove l'accuratezza dei dati è fondamentale.
* Gli oracoli recuperano e verificano i dati esterni per le blockchain e gli smart contract attraverso metodi quali API web o feed di dati di mercato. Il tipo di dati richiesti dagli smart contract può includere informazioni sui prezzi, informazioni meteo o persino la generazione di numeri casuali per il gioco d'azzardo. L'utilizzo degli oracoli consiste nell'interrogare la fonte di dati per ottenere informazioni specifiche e successivamente connettersi a tale fonte per interfacciarsi tra la blockchain e il feed di dati. Di conseguenza, i contratti intelligenti possono essere eseguiti in base alle informazioni specifiche provenienti dal flusso di dati.
* Questi consentono la creazione degli hybrid smart contracts, combinando una infrastruttura on-chain con una off-chain e quindi fornendo calcolo a reti decentralizzate di oracoli (quindi, multipli per evitare un singolo punto di fallimento e anzi estendere la persistenza e la ridondanza della rete a tutti i nodi). Queste reti sono decentralized oracle networks (DONs).
* I DON possono essere utilizzati per collegare vari tipi di dati esterni a e da blockchain, consentendo di scrivere contratti intelligenti ibridi attorno a quei dati specifici. Alcuni dei tipi di dati iniziali resi accessibili includono:
  + Price Feeds - dati sui prezzi delle attività aggregati da centinaia di borse, ponderati per il volume e ripuliti da outlier e wash trading.
  + Proof of Reserve - dati aggiornati sugli attuali saldi di riserva a sostegno degli asset tokenizzati, come le riserve di BTC che garantiscono WBTC o il conto bancario in USD che garantisce TUSD.
  + Qualsiasi API - dati premium provenienti da API protette da password, che vanno dalle previsioni del tempo e dai risultati delle partite sportive alle informazioni provenienti da un backend aziendale e da una rete IoT.
  + Blockchain Middleware - livello di astrazione per un sistema fuori catena per leggere e scrivere dati da e verso smart contract su qualsiasi rete blockchain.
* Per comprendere meglio la differenza tra i componenti on-chain e off-chain, identifichiamo i ruoli distinti di ciascuno:
* On-Chain: Blockchain
  + Mantenere un libro mastro persistente che fornisce una custodia autorevole delle attività degli utenti e interagisce con le chiavi private.
  + Eseguire il regolamento finale elaborando transazioni irreversibili che trasferiscono valore tra gli utenti.
  + Fornire la risoluzione delle controversie e i guardrail per garantire il corretto funzionamento dei servizi off-chain eseguiti da un DON.
* Off-Chain: Rete decentralizzata di Oracle
  + Recuperare, convalidare, proteggere e consegnare dati da API esterne a smart contract in esecuzione su blockchain e soluzioni di livello 2
  + Eseguire vari tipi di calcoli per gli smart contract in esecuzione su blockchain e soluzioni layer-2.
  + Trasmettere le uscite del codice degli smart contract ad altre blockchain o a sistemi esterni.
* I DON possono eseguire una serie di calcoli fuori catena per conto dello smart contract, per aiutarlo a ottenere input specifici o a generare determinate caratteristiche non possibili sulla sua specifica blockchain, come la privacy, la scalabilità e l'equità degli ordini. Alcune delle computazioni off-chain attuali e future possibili attraverso i DON includono:
  + Keeper Network - bot di automazione che eseguono compiti di manutenzione regolare per lo smart contract, svegliandolo quando deve eseguire funzioni chiave sulla catena.
  + Off-Chain Reporting (OCR) - aggregazione scalabile delle risposte dei nodi oracolo in un DON che vengono poi consegnate sulla catena in un'unica transazione per ridurre i costi sulla catena.
  + Scalable Computation - esecuzione di contratti ad alta velocità e a basso costo per smart contract autonomi, che si sincronizza periodicamente sulla catena utilizzando la tecnologia layer-2 esistente.
  + Verifiable Randomness Function (VRF) - generazione di numeri casuali sicura e verificabile, supportata da prove crittografiche che dimostrano l'integrità del processo.
  + Data and Computation Privacy - calcolo oracolare che preserva la privacy e che rende i dati sensibili disponibili in modo confidenziale agli smart contract utilizzando prove a conoscenza zero (DECO), hardware fidato (Town Crier), calcolo multi-party sicuro e/o utilizzando comitati DON selezionati.
  + Fair Sequencing Services (FSS) - ordinamento decentralizzato delle transazioni basato su una nozione predefinita di equità, che impedisce il frontrunning e il miner extractable value (MEV).
  + On-Chain Contract Privacy - privacy delle transazioni per uno smart contract attraverso una decorrelazione tra la logica del contratto e l'output del regolamento, utilizzando il DON per ritrasmettere la comunicazione tra le due parti, come nel caso di Mixicles.

Un oracolo blockchain è un pezzo sicuro di middleware che facilita la comunicazione tra le blockchain e qualsiasi sistema esterno alla catena, compresi i fornitori di dati, le API web, i backend aziendali, i fornitori di cloud, i dispositivi IoT, le firme elettroniche, i sistemi di pagamento, altre blockchain e altro ancora. Questi svolgono diverse funzioni chiave:

* Ascoltare - monitorare la rete blockchain per verificare eventuali richieste di dati fuori catena da parte di utenti o smart contract.
* Estrarre - recuperare i dati da uno o più sistemi esterni, come le API off-chain ospitate su server web di terze parti.
* Formattare - formattare i dati recuperati da API esterne in un formato leggibile dalla blockchain (input) e/o rendere i dati della blockchain compatibili con un'API esterna (output).
* Validare - generare una prova crittografica che attesti le prestazioni di un servizio oracolo utilizzando qualsiasi combinazione di firma dei dati, firma delle transazioni blockchain, firme TLS, attestazioni di Trusted Execution Environment (TEE) o prove a conoscenza zero.
* Computare - eseguire qualche tipo di calcolo sicuro fuori dalla catena per lo smart contract, come ad esempio calcolare una mediana da più invii dell'oracolo o generare un numero casuale verificabile per un'applicazione di gioco.
* Broadcast - firma e trasmette una transazione sulla blockchain per inviare i dati e qualsiasi prova corrispondente sulla catena per il consumo da parte dello smart contract.
* Output (opzionale) - inviare dati a un sistema esterno in seguito all'esecuzione di uno smart contract, come ad esempio trasmettere istruzioni di pagamento a una rete di pagamento tradizionale o attivare azioni da un sistema cyber-fisico.

Per svolgere le funzioni sopra descritte è necessario che il sistema oracolo operi contemporaneamente sia sulla blockchain che al di fuori di essa. La componente on-chain serve a stabilire una connessione alla blockchain (per ascoltare le richieste), trasmettere dati, inviare prove, estrarre dati della blockchain e potenzialmente eseguire calcoli sulla blockchain. La componente off-chain serve per elaborare le richieste, recuperare e formattare i dati esterni, inviare i dati della blockchain a sistemi esterni ed eseguire calcoli off-chain per una maggiore scalabilità, privacy, sicurezza e vari altri miglioramenti degli smart contract.



Riferimento: <https://blog.chain.link/what-is-the-blockchain-oracle-problem/>

Esistono diverse forme di oracoli, tra cui:

* Gli *oracoli hardware* sono sensori integrati in oggetti fisici tangibili. Gli esempi principali sono la tracciabilità della catena di approvvigionamento con l'uso di tag RFID per fornire dati come le condizioni ambientali dei prodotti alla blockchain.
* Gli *oracoli software* sono la forma più comune che attinge i dati da fonti di terze parti, come le API web, e possono includere informazioni del mondo reale come lo stato dei voli e i dati meteorologici.
* Gli *oracoli di consenso* rappresentano un passo avanti verso gli oracoli decentralizzati e si basano sull'aggregazione di dati provenienti da diversi oracoli con metodi proprietari per determinarne l'autenticità e l'accuratezza.
* Gli *oracoli in entrata (inbound oracles)* riflettono gli scenari "se questo accade allora fai quello" associati agli oracoli software, come ad esempio "se questo prezzo è raggiunto da un asset, allora attiva una vendita".
* Gli *oracoli in uscita (outbound oracles)* consentono agli smart contract di inviare dati a fonti esterne alla rete blockchain su cui si trovano e sono anch'essi oracoli software.

Qui si parla di *Oracle Problem*, in quanto un oracolo fornisce agli smart contract le risposte alle domande sul mondo. Nella maggior parte dei casi, senza un oracolo che fornisca informazioni, non ci sarebbe modo per uno smart contract di conoscere le cose che deve sapere per svolgere il suo lavoro.

* Poiché un oracolo determina ciò che uno smart contract vede (cioè controlla gli input dello smart contract), ha anche il potere di controllare ciò che lo smart contract fa in risposta a questi input. Ciò significa che gli oracoli possiedono un'enorme quantità di potere quando si tratta di smart contract (specialmente in contesti di mercato predittivo). Se l'oracolo è compromesso, lo è anche l'intero contratto; le blockchain non possono ricevere dati da o inviare dati a sistemi esterni come funzionalità integrata.
* Le blockchain non sono adatte a rispondere a domande che si spingono nel regno della soggettività o che richiedono dati esterni non facilmente accessibili a tutti i nodi della rete. Ad esempio, una semplice domanda come "Qual è il prezzo di mercato del Bitcoin?" o "Che tempo fa a New York?" può suscitare un'ampia gamma di risposte diverse che possono variare a seconda della fonte di dati utilizzata e del momento in cui vengono richiesti. La domanda diventa quindi: qual è la risposta corretta e come si può verificare che sia vera?
* L'introduzione della soggettività nel livello di base della blockchain apre il vaso di Pandora a tutta una serie di problemi di sicurezza, affidabilità e governance, mettendo a rischio la stessa proposta di valore che le blockchain intendono fornire.
* È estremamente difficile gestire e far rispettare la qualità dei dati off-chain inviati dai nodi della blockchain, poiché chiunque può gestire un nodo in modo pseudo-anonimo e inviare risposte, anche se non è disposto ad acquistare un abbonamento a un'API off-chain di alta qualità. Se la qualità dei dati fosse imposta, la blockchain avrebbe un limite superiore inferiore alla decentralizzazione, poiché i costi di gestione dei nodi aumenterebbero per ogni nuovo lavoro di oracolo sulla rete, incidendo sulla sicurezza di tutte le altre applicazioni in esecuzione su quella particolare blockchain.
* Un'altra grande preoccupazione è la scalabilità. Ogni volta che una nuova fonte di dati deve essere aggiunta alla rete o un metodo di aggregazione dei dati esistente deve essere adattato, è necessario un massiccio coordinamento di governance sociale per far sì che ogni nodo della rete sia d'accordo e aggiorni il proprio software. L'aggiunta di costi generali di governance porta a un aumento dell'attrito, a un rallentamento dello sviluppo delle funzionalità fondamentali della blockchain (come PoS e sharding) e a forti limiti all'innovazione di Oracle. In definitiva, maggiore è la complessità del livello di base della blockchain, maggiore è la superficie di attacco e il rischio per tutte le applicazioni che vi girano sopra.

L'intero scopo di uno smart contract è quello di ottenere il determinismo attraverso l'esecuzione tecnologica dei termini del contratto, in contrapposizione all'esecuzione probabilistica effettuata dall'uomo. Per raggiungere questo obiettivo, la blockchain non può avere un singolo punto di guasto, caratteristica che deve essere estesa all'oracolo se si vuole mantenere il determinismo degli smart contract end-to-end. Perché far funzionare un contratto multimilionario come smart contract su una blockchain completamente decentralizzata se un singolo oracolo centralizzato può controllare gli input che determinano l'esito del contratto (diventano Single Point of Failure)?

Esistono sistemi come Chainlink in grado di portare determinismo all’oracle layer, che ha sviluppato una rete di reti di oracoli decentralizzati (DON), con ogni DON che comporta una combinazione di più tecniche di sicurezza necessarie per servire un particolare caso d'uso. Alcune caratteristiche utili:

* Open-source - il fatto di essere una tecnologia open-source consente alla più ampia comunità blockchain di verificare in modo indipendente la sicurezza e l'affidabilità del codice sorgente e delle funzioni di Chainlink, nonché di contribuire al suo miglioramento.
* Adattatori esterni - la possibilità per i nodi di memorizzare in modo sicuro le chiavi API e di gestire i login degli account consente agli smart contract di recuperare dati da qualsiasi sistema e API esterni, compresi quelli protetti da password/credenziali.
* Decentralizzazione - l'impiego della decentralizzazione a livello di nodi e di fonti di dati assicura che nessun nodo o fonte di dati sia un singolo punto di guasto, fornendo agli utenti forti garanzie sulla disponibilità dei dati, sulla loro puntualità e sulla loro resistenza alla manipolazione.
* Firma dei dati - il fatto che i nodi firmano crittograficamente i dati che forniscono agli smart contract consente agli utenti di identificare quali nodi hanno inviato i dati e di esaminare la loro storia passata per determinare la qualità delle loro prestazioni.
* Accordi di servizio - l'utilizzo di accordi vincolanti on-chain tra lo smart contract richiedente e il fornitore dell'oracolo, che delineano i termini del servizio dell'oracolo e le penalità/premi per le prestazioni, fornisce agli utenti garanzie applicabili sulla qualità delle loro richieste di dati off-chain.
* Sistemi di reputazione - l'alimentazione dei dati firmati sulla catena nei sistemi di reputazione consente agli utenti di prendere decisioni informate su quali nodi sono validi e quali no, sulla base di una serie di metriche come i lavori eseguiti con successo, l'elenco dei clienti serviti, il tempo medio di risposta, ecc.
* Servizi di certificazione - consentire ai nodi di aumentare la loro sicurezza e affidabilità ottenendo un numero qualsiasi di certificazioni può fornire agli utenti garanzie aggiuntive come KYC, posizione geografica del nodo, revisioni di sicurezza della sua infrastruttura e altro ancora.
* Crittografia e hardware avanzati - fornire flessibilità per la crittografia più avanzata (come le prove a conoscenza zero) e l'hardware (come gli ambienti di esecuzione fidati) consente agli oracoli di svolgere funzioni aggiuntive come dimostrare l'origine dei dati (ad esempio, dati specifici provengono da un server specifico), mantenere i dati riservati, eseguire calcoli fuori catena e altro ancora.

## Linguaggi per smart contract: Solidity

Solidity è un linguaggio ad alto livello usato per implementare gli smart contract designato per essere utilizzato nella Ethereum Virtual Machine (EVM), supportando l’ereditarietà, librerie, tipi definiti dall’utente ed altre caratteristiche, essendo linguaggio staticamente tipizzato. Si ispira a C++, Python, JavaScript e simili.

Si può scriverne direttamente codice al link: <https://remix.ethereum.org>

### Esempi di codice e passi base

La prima cosa da fare è dichiararsi la versione da utilizzare, con la direttiva *pragma* e si aggiunge la licenza di utilizzo.

//SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

Di seguito l’esempio semplice di un contratto, creando due funzioni di *get* e *set* e un costruttore nella sintassi specifica:

pragma solidity ^0.8.0;

contract MyContract{

    string value;

    constructor() public{

        value = "myValue";

    }

    function get() public view returns(string memory){

        return value;

    }

    function set(string memory \_value) public{

        value = \_value;

    }

}

Esistono diversi tipi di Solidity, ognuno dei quali ha una funzione specifica.

* booleano (*bool*): è utilizzato per rappresentare i valori booleani, ovvero vero o falso. In Solidity, il valore "true" è rappresentato dal numero 1 e il valore "false" dal numero 0.
* intero (*int*): viene utilizzato per rappresentare numeri interi positivi o negativi. In Solidity, esistono diversi tipi di dati interi con dimensioni variabili, a seconda del numero di bit utilizzati per rappresentare il valore. Per gli interi solamente positivi, avremo *uint* (*unsigned int*) e ce ne sono diversi: uint, uint8, uint16, uint24, uint32, uint64, uint128 e uint256
* *address*, che indica un indirizzo pubblico per inviare Ether
* stringa (*string*): il tipo di dati stringa viene utilizzato per rappresentare stringhe di caratteri. In Solidity, le stringhe vengono codificate in UTF-8 e la loro lunghezza massima è di 2^256 caratteri. Si basano su Byte, ma le stringhe si usano per il testo, mentre i Byte grezzi per memorizzarne ulteriori. È inoltre possibile utilizzare byte1, byte2, byte3 fino a byte32. Questi sono usati per lo stesso scopo, per la memorizzazione di dati di testo e di byte ma usano meno gas, il che è ottimo per gli utenti perché dovranno pagare meno ether per interagire con quelle variabili.
* *array*: il tipo di dati array viene utilizzato per rappresentare una serie di valori dello stesso tipo. In Solidity, esistono diversi tipi di array, tra cui gli array statici e gli array dinamici. Come per altri linguaggi, si dichiarano con le quadre
* *mapping*: il tipo di dati mapping viene utilizzato per rappresentare una corrispondenza tra una chiave e un valore. In Solidity, i mapping sono utilizzati spesso per creare strutture dati complesse.
* *struct*: il tipo di dati struct viene utilizzato per definire una struttura dati personalizzata che può contenere diversi tipi di dati.

Quando si esegue un contratto, si pagherà del gas (tassa della blockchain Ethereum) quando viene fatto il deploy del contatto specifico. Per esempio, una funzione di lettura come nel codice che segue, costerà solo quando chiamo *retrieve()*.

Immagine che contiene testo

Descrizione generata automaticamente

Un esempio di *struct* oppure di *array*:

    struct People{

        uint256 favoriteNumber;

        string name;

    }

    uint256 public favoriteNumbersList;

    People[] public people;

Distinguiamo:

* *memory*, che permette di salvare una variabile temporaneamente. Questa viene usata anche per indicare come si comporti una locazione “insicura” (ad esempio, strutture come array, struct e mappings. In questo modo, diciamo al compilatore esattamente come comportarsi quando non si sa esattamente quanta memoria allocare)
* *storage*, che la salva permanentemente e si vede anche al di fuori della funzione

Un esempio di seguito di codice che usa una struttura *mapping* per salvare e “mappare” un intero ad una stringa:

//SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

contract MyContract{

    uint256 public favoriteNumber;

    //People public person = People({favoriteNumber: 2, name : "Gabriel"});

    struct People{

        uint256 favoriteNumber;

        string name;

    }

    People[] public people; //static array

    mapping (string => uint256) public nameToFavoriteNumber; //dictionary to map name to a specific number

    //view, pure

    function store (uint256 \_favoriteNumber) public {

        favoriteNumber = \_favoriteNumber;

    }

    function retrieve() public view returns(uint256){

        return favoriteNumber;

    }

    //calldata, memory (temporary variable, like "name"), storage (permanent variable, exists even outside the function)

    function addPerson(string memory \_name, uint256 \_favoriteNumber) public{

        people.push(People(\_favoriteNumber, \_name));

        nameToFavoriteNumber[\_name]=\_favoriteNumber;

    }

}

SI può inoltre cambiare l’ambiente di esecuzione nella sezione di compilazione, ad esempio:

* Injected Provider setta (tramite un wallet come Metamask) l’utilizzo di un servizio esterno per interagire con lo smart contract che stiamo scrivendo,

È possibile che un file contenga più contratti, poi scegliendo su quale fare il deploy facilmente in fase di esecuzione. Come si vede, si può fare in questo modo, importando il codice precedente:

// SPDX-License-Identifier: MIT

pragma solidity 0.8.8;

import "./SimpleStorage.sol";

contract StorageFactory{

    SimpleStorage[] public simpleStorageArray;

    function createSimpleStorageContract() public{

        SimpleStorage simpleStorage = new SimpleStorage();

    }

}

Quando si importa una funzione, prendiamo subito la sua ABI (Application Binary Interface) nel contesto dell'informatica è un'interfaccia tra due moduli di programma, spesso tra sistemi operativi e programmi utente.

Gli smart contract scritti in linguaggi di alto livello come Solidity o Vyper devono essere compilati in bytecode eseguibile EVM; quando uno smart contract viene distribuito, questo bytecode viene memorizzato sulla blockchain ed è associato a un indirizzo. Per Ethereum ed EVM, uno smart contract è proprio questa sequenza di bytecode. Per accedere alle funzioni definite nei linguaggi di alto livello, gli utenti devono tradurre i nomi e gli argomenti in rappresentazioni di byte affinché il codice byte possa lavorare con esse.

Per interpretare i byte inviati in risposta, gli utenti devono riconvertire le tuple di valori di ritorno definiti nei linguaggi di alto livello. I linguaggi che compilano per l'EVM mantengono convenzioni rigorose su queste conversioni, ma per eseguirle è necessario conoscere i nomi e i tipi precisi associati alle operazioni. L'ABI documenta questi nomi e tipi in modo preciso, in un formato facilmente analizzabile, rendendo le traduzioni tra le chiamate di metodo volute dall'uomo e le operazioni degli smart-contract scopribili e affidabili.

È molto simile all'API (Application Program Interface), una rappresentazione leggibile dall'uomo dell'interfaccia di un codice. L'ABI definisce i metodi e le strutture utilizzate per interagire con il contratto binario, proprio come fa l'API, ma a un livello inferiore. L'ABI indica al chiamante della funzione di codificare le informazioni necessarie, come le firme delle funzioni e le dichiarazioni delle variabili, in un formato che l'EVM può comprendere per chiamare la funzione in bytecode; questa operazione è chiamata codifica ABI. La codifica ABI è per lo più automatizzata, gestita da compilatori come REMIX o da portafogli che interagiscono con la blockchain. L'ABI dei contratti è rappresentato in formato JSON. Esistono specifiche chiare su come codificare e decodificare un contratto ABI.

Il JSON di una ABI è come segue:

Immagine che contiene testo

Descrizione generata automaticamente

Riferimento: <https://www.quicknode.com/guides/ethereum-development/smart-contracts/what-is-an-abi/>

Un esempio di ereditarietà rispetto al codice precedente avviene con la keyword *is* per indicare il fatto di essere sottoclasse e ridefiniamo una funzione precedente (*overriding*) con la keyword *override*.

// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

import "./SimpleStorage.sol";

contract ExtraStorage is SimpleStorage{

    function store(uint256 \_favoriteNumber) public override{

        favoriteNumber = \_favoriteNumber + 5;

    }

}

Possiamo settare una funzione per fare in modo ripaghi nelle valute Ethereum. Di seguito un recap:

Immagine che contiene tavolo

Descrizione generata automaticamente

Riferimento: <https://www.alchemy.com/gwei-calculator>

Similmente, possono essere introdotte due keywords:

* *payable* per fare in modo una transazione trasferisca delle valute
* *require* per fare in modo vengano correttamente eseguiti dei controlli e prevenire transazioni inutili
* *library,* simili ai contratti ma non si possono dichiarare variabili di stato oppure inviare degli ether

Possiamo vedere l’utilizzo di un oracolo con l’utilizzo di un metodo di conversione da Ether a dollari con un indirizzo di test e relativa conversione.

// SPDX-License-Identifier: MIT

pragma solidity ^0.8.8;

import "@chainlink/contracts/src/v0.8/interfaces/AggregatorV3Interface.sol";

contract FundMe {

    function fund() public payable {

        require(msg.value.getConversionRate() >= MINIMUM\_USD, "You need to spend more ETH!");

        // require(PriceConverter.getConversionRate(msg.value) >= MINIMUM\_USD, "You need to spend more ETH!");

        addressToAmountFunded[msg.sender] += msg.value;

        funders.push(msg.sender);

    }

    function getVersion() public view returns (uint256){

        // ETH/USD price feed address of Sepolia Network.

        AggregatorV3Interface priceFeed = AggregatorV3Interface(0x694AA1769357215DE4FAC081bf1f309aDC325306);

        return priceFeed.version();

    }

}

Un esempio di library è come segue, seguendo la logica di sopra:

// SPDX-License-Identifier: MIT

pragma solidity ^0.8.8;

import "@chainlink/contracts/src/v0.8/interfaces/AggregatorV3Interface.sol";

// Why is this a library and not abstract?

// Why not an interface?

library PriceConverter {

    // We could make this public, but then we'd have to deploy it

    function getPrice() internal view returns (uint256) {

        // Sepolia ETH / USD Address

        // https://docs.chain.link/data-feeds/price-feeds/addresses#Sepolia%20Testnet

        AggregatorV3Interface priceFeed = AggregatorV3Interface(0x694AA1769357215DE4FAC081bf1f309aDC325306);

        (, int256 answer, , , ) = priceFeed.latestRoundData();

        // ETH/USD rate in 18 digit

        return uint256(answer \* 10000000000);

        // or (Both will do the same thing)

        // return uint256(answer \* 1e10); // 1\* 10 \*\* 10 == 10000000000

    }

    // 1000000000

    function getConversionRate(uint256 ethAmount)

        internal

        view

        returns (uint256)

    {

        uint256 ethPrice = getPrice();

        uint256 ethAmountInUsd = (ethPrice \* ethAmount) / 1000000000000000000;

        // or (Both will do the same thing)

        // uint256 ethAmountInUsd = (ethPrice \* ethAmount) / 1e18; // 1 \* 10 \*\* 18 == 1000000000000000000

        // the actual ETH/USD conversion rate, after adjusting the extra 0s.

        return ethAmountInUsd;

    }

}

Similmente, possiamo rappresentare delle vulnerabilità matematiche poi risolte con questo esempio:

// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

contract SafeMathTester{

    uint8 public bigNumber = 255; //unchecked --> check for the max number to not fail the single transaction

    function add() public{

        bigNumber = bigNumber + 1;

    }

}

/\*

In 0.8 above:

    function add() public{

        unchecked {bigNumber = bigNumber + 1;}

    }

The code might be more gas efficient

\*/

In Solidity, la parola chiave *modifier* viene utilizzata per definire un pezzo di codice riutilizzabile che può essere applicato alle funzioni, consentendo l'implementazione di funzionalità comuni di validazione, autorizzazione o altro che possono essere condivise tra più funzioni.

Inoltre:

In Solidity, le funzioni receive e fallback sono funzioni speciali utilizzate per gestire le transazioni in arrivo a un contratto quando nessun'altra funzione corrisponde alla firma della funzione.

La funzione receive ha la seguente firma:

*receive() external payable {*

*// codice per gestire le transazioni in entrata*

*}*

È una funzione speciale che viene chiamata automaticamente quando un contratto riceve etere senza una chiamata di funzione o quando un contratto riceve etere e la funzione chiamata non è contrassegnata come pagabile. La funzione receive deve essere contrassegnata come pagabile per poter ricevere etere e può essere definita solo una volta in un contratto.

La funzione di fallback, invece, ha la seguente firma:

*fallback() external payable {*

*// codice per gestire le transazioni in entrata*

*}*

È una funzione speciale che viene chiamata automaticamente quando un contratto riceve una transazione che non corrisponde a nessuna delle sue firme di funzione. A differenza della funzione receive, la funzione fallback non deve essere contrassegnata come pagabile e può essere definita più volte all'interno di un contratto.

Sia la funzione *receive* che la funzione *fallback* possono essere utilizzate per gestire le transazioni in arrivo a un contratto, ma la funzione receive è preferita per gestire l'etere in arrivo, mentre la funzione fallback è utilizzata per altri tipi di transazioni, come l'invio di dati a un contratto. È importante notare che nelle versioni di Solidity successive alla 0.6.0, si raccomanda di usare receive() invece di fallback() per gestire gli ether in entrata.

Nota di margine 🡪 \_; // this underscore indicates where the function code should be executed

Fino ad ora è stato usato Remix Ethereum per compilare; tuttavia:

* può solo gestire degli smart contract
* non si può integrare con altre parti di un progetto
* non può salvare file in locale senza un plugin
* tutte le funzionalità custom richiedono un plugin

Ora useremo *Hardhat*, basato su JavaScript.

È uno strumento open-source che fornisce una suite di funzioni e utilità per rendere il processo di sviluppo e di test più veloce, più facile e più snello.

Hardhat supporta una serie di funzioni per la creazione, il test e la distribuzione di contratti intelligenti. Alcune di queste funzioni includono:

* Compilazione di contratti intelligenti: Hardhat consente agli sviluppatori di compilare i loro contratti smart Solidity in bytecode che possono essere distribuiti sulla rete Ethereum.
* Test dei contratti: Hardhat fornisce una suite di strumenti di test che facilitano la scrittura e l'esecuzione di test per i contratti intelligenti.
* Debug: Hardhat include un debugger integrato che consente agli sviluppatori di analizzare il codice e di verificare i cambiamenti di stato durante l'esecuzione.
* Stima del gas: Hardhat fornisce uno strumento di stima del gas che può aiutare gli sviluppatori a ottimizzare i loro contratti per l'utilizzo del gas.
* Script di distribuzione: Hardhat consente agli sviluppatori di scrivere script che automatizzano la distribuzione dei contratti intelligenti sulla rete Ethereum.

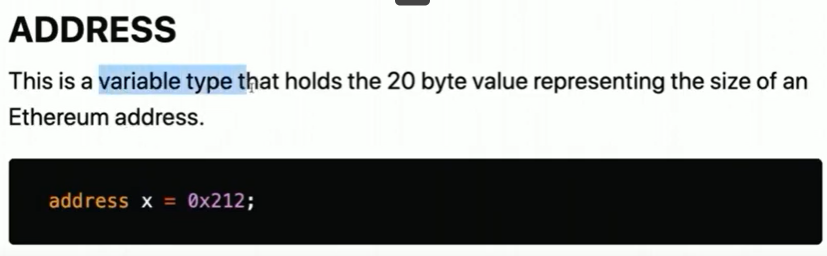
Oltre a queste caratteristiche, Hardhat si integra anche con altri strumenti e framework Ethereum popolari, come Truffle, Web3.js e Ethers.js. In questo modo è facile utilizzare Hardhat insieme a questi altri strumenti o migrare da uno strumento all'altro, se necessario.

Comandi base:

* Aggiunta al progetto 🡪 yarn add hardhat
* Compilazione 🡪 yard hardhat compile
* Deploy 🡪 yarn hardhat deploy
  + Su una testnet 🡪 yard hardhat deploy --network rinkeby
* Test 🡪 yarn hardhat test
* Coverage 🡪 yarn hardhat coverage

### Solidity in a nutshell

* All’inizio di un file:
  + Licenza 🡪 // SPDX-License-Identifier: MIT
  + Versione di Solidity 🡪 pragma solidity ^0.8.17;
* Gli indirizzi sono di tipo *address* ed hanno 20 byte



* *mapping*

Immagine che contiene testo

Descrizione generata automaticamente

* *memory* 🡪 Variabile temporanea che è in memoria ed esiste mentre la funzione viene chiamata
* *storage* 🡪 Variabile di stato (quindi, memorizzate permanentemente nella memoria del contratto) memorizzata sulle blockchain
  + Diversamente dalle funzioni, le variabili di stato non possono essere sovrascritte dichiarandole nuovamente nel contratto figlio.
* *calldata* 🡪 Locazione speciali di memoria che contengono argomenti di funzione
* *payable* 🡪 La funzione e gli indirizzi possono ricevere ether nel contratto
* *view* 🡪 Lo stato della funzione non sarà cambiato
* *pure* 🡪 La funzione dichiara che nessuna variabile di stato sarà cambiata o letta
* *modifier* 🡪 Codice eseguito prima o dopo la chiamata di una funzione. Vengono usati per
  + Restringere l’accesso (controllando ad esempio il chiamante sia il proprietario del contratto)
  + Validare gli input
  + Proteggersi dagli attacchi di reentrancy
* *event* 🡪 Permette il logging sulla blockchain Ethereum; spesso usati per aggiornare le interfacce ed ascoltare cosa succede sulla blockchain
* Modificatori
  + *public* - tutti possono accedervi
  + *external* - Non si può accedere internamente, solo esternamente
  + *internal* - solo questo contratto e i contratti da esso derivati possono accedervi
  + *private* - si può accedere solo da questo contratto
* Funzione e scrittura
  + *function nome (parametri eventuali) modificatori altre (virtual/pure/etc.) returns (tipo memory)*
* Ereditarietà
  + I contratti ereditano usando la keyword *is*
  + La funzione che verrà sovrascritta da un contratto figlio deve essere dichiarata come *virtual*
  + Le funzioni che sovrascrivono una funzione genitore devono utilizzare la keyword *override*.
  + I contratti padre possono essere richiamati direttamente o utilizzando la parola chiave *super*.
  + Utilizzando la parola chiave *super*, verranno richiamati tutti i contratti padre immediati.
* Invio Ether (tre funzioni: *transfer, end, call*)
  + Come inviare Ether?
    - È possibile inviare Ether ad altri contratti tramite
      * *transfer* (2300 gas, lancia errore)
      * *send* (2300 gas, restituisce bool)
      * *call* (inoltrare tutto il gas o impostare il gas, restituisce bool)
  + Come ricevere Ether?
    - Un contratto che riceve Ether deve avere almeno una delle funzioni seguenti
      * *receive() external payable*
      * *fallback() external payable*
      * *receive()* viene chiamata se msg.data è vuoto, altrimenti viene chiamata fallback().
  + Quale metodo si dovrebbe utilizzare?
    - *call* in combinazione con la protezione da rientranze è il metodo consigliato da utilizzare dopo dicembre 2019.
  + Per evitare la rientranza, occorre
    - effettuando tutte le modifiche allo stato prima di chiamare altri contratti
    - utilizzando il modificatore di guardia di rientranza
* fallback 🡪 funzione speciale che viene eseguita quando
  + viene chiamata una funzione che non esiste o
  + L'Etere viene inviato direttamente a un contratto, ma receive() non esiste o msg.data non è vuoto.
  + fallback ha un limite di 2300 gas quando viene chiamata da transfer o send.
* Quando si chiama una funzione, i primi 4 byte di calldata specificano quale funzione chiamare.
  + Questi 4 byte sono chiamati selettori di funzione.
  + Prendiamo ad esempio il codice qui sotto. Utilizza call per eseguire il trasferimento su un contratto all'indirizzo addr.
* addr.call(abi.encodeWithSignature("transfer(address,uint256)", 0xSomeAddress, 123))
  + I primi 4 byte restituiti da abi.encodeWithSignature(....) sono il selettore di funzione. Forse si può risparmiare una piccola quantità di gas se si precompila e si mette in linea il selettore di funzioni nel codice?
* Ecco come viene calcolato il selettore di funzioni.

// Identificatore di licenza SPDX: MIT

pragma solidity ^0.8.17;

contract FunctionSelector {

/\*

"transfer(indirizzo,uint256)"

0xa9059cbb

"transferFrom(indirizzo,indirizzo,uint256)"

0x23b872dd

\*/

function getSelector(string calldata \_func) external pure returns (bytes4) {

return bytes4(keccak256(bytes(\_func));

}

}

* La chiamata del contratto si ha:
  + Il modo più semplice è chiamarlo, come A.foo(x, y, z).
  + Un altro modo per chiamare altri contratti è quello di utilizzare la chiamata di basso livello con call. Questo metodo non è raccomandato.
* I contratti possono essere creati da altri contratti utilizzando la parola chiave new. Dalla 0.8.0, la nuova parola chiave supporta la funzione create2 specificando le opzioni di sale.
* *Library* 🡪 Le librerie sono simili ai contratti, ma non è possibile dichiarare alcuna variabile di stato e non è possibile inviare etere.
  + Una libreria è incorporata nel contratto se tutte le funzioni della libreria sono interne.
  + In caso contrario, la libreria deve essere distribuita e poi collegata prima che il contratto venga distribuito.
* *keccak256* 🡪 calcola l'hash Keccak-256 dell'input. Alcuni casi d'uso sono:
  + Creazione di un ID univoco deterministico da un input
  + Schema Commit-Reveal
  + Firma crittografica compatta (firmando l'hash invece di un input più grande)
* Alcune tecniche di risparmio di gas.
  + Sostituzione della memoria con i dati di chiamata
  + Caricamento della variabile di stato in memoria
  + Sostituzione del ciclo for i++ con ++i
  + Caching degli elementi dell'array
  + Cortocircuito
* L'overflow e l'underflow dei numeri in Solidity 0.8 generano un errore. Questo può essere disabilitato usando unchecked.
  + Disabilitando il controllo dell'overflow e dell'underflow, si risparmia gas.

## Framework JavaScript per interazione blockchain

### Ethers.js

Ethers.js è uno degli strumenti più necessari per gli sviluppatori che cercano di costruire una dApp o un'applicazione basata su qualsiasi Blockchain nella loro fase iniziale di sviluppo. Fornisce un'interfaccia semplice che rende il lavoro dello sviluppatore estremamente facile ed efficace. Con il suo aiuto possono interagire facilmente con la Blockchain sottostante e possono anche fare richieste alla Blockchain e generare risposte attraverso di essa.

Esempi di codice della sezione presenti nella repo: <https://github.com/dappuniversity/ethers_examples>

Alcune caratteristiche rilevanti:

* API facile da usare: Ethers.js fornisce un'API semplice ma potente che consente agli sviluppatori di interagire facilmente con la rete Ethereum e di eseguire operazioni comuni. È leggera e la sua API è abbastanza semplice da consentire a qualsiasi sviluppatore di iniziare il proprio percorso di sviluppo.
* Interfaccia semplice e facile da interagire: Ethers.js riduce la complessità della rete Ethereum, rendendo più facile per gli sviluppatori concentrarsi sulla creazione delle loro applicazioni. Anche altri framework come Web3.js sono validi, ma la loro interfaccia complessa non è facile da comprendere e utilizzare per i principianti.
* Ampiamente utilizzato dalla comunità di Ethereum: È popolare all'interno della comunità di Ethereum, il che rende facile per gli sviluppatori trovare e cercare la sua documentazione e le sue pratiche. Inoltre, aiuta a condividere le proprie conoscenze con gli altri.
* Supporto sia per Node.js che per i browser web: Ethers.js supporta sia Node.js che i browser web, rendendolo uno strumento versatile per lo sviluppo di Ethereum.

Ethers.js è caratterizzato da un bundle di dimensioni ridotte, da una documentazione ampia e semplice e da una struttura API di facile utilizzo. Inoltre, è intuitivo e semplice da usare. Inoltre, oltre a JavaScript, ethers.js supporta TypeScript (TS). Tutti questi vantaggi, uniti alle caratteristiche sopra elencate, rendono ethers.js una libreria molto interessante per molti sviluppatori Web3.

Vediamo una sintesi dei principali vantaggi di ethers.js:

* Dimensioni minime - ethers.js è minuscolo, solo 88 KB compressi e 284 KB non compressi.
* Include un'ampia documentazione.
* Viene fornito con un'ampia raccolta di casi di test mantenuti.
* Ethers.js include i file di definizione e i sorgenti completi di TS - è completamente pronto per TypeScript.
* Viene fornito con una licenza MIT open-source che include tutte le dipendenze.

Oltre a questi vantaggi specifici di ethers.js, imparare a usare ethers.js porta alcuni vantaggi universali. Dopo tutto, la blockchain è qui per restare ed è pronta a cambiare radicalmente il modo in cui il mondo opera. Pertanto, potete utilizzare questo tutorial su ethers.js sapendo che vi aiuterà a imparare a diventare parte di questa soluzione.

Inoltre, alcuni degli esempi più comuni di ethers.js riguardano la creazione di whale alert (dati in tempo reale sulle transazioni blockchain), la costruzione di bot automatizzati, il monitoraggio delle collezioni NFT, le notifiche di gioco Web3, ecc. In definitiva, quando si ascoltano gli eventi della catena con ethers.js o con altri strumenti affidabili, l'obiettivo principale è quello di eseguire automaticamente azioni in risposta a specifici eventi della catena. Quindi, il vostro obiettivo deve essere quello di scegliere uno strumento che vi permetta di farlo in modo efficace ed efficiente.

Un piccolo esempio molto semplice.

* Quindi, in prima battuta, bisogna assicurarsi che il file NodeJS utilizzi ethers.js. Poi, bisogna importare l'interfaccia binaria dell'applicazione (ABI), che è specifica per ogni smart contract. Detto questo, la funzione asincrona "getTransfer" merita la massima attenzione. Dopo tutto, quest'ultima si occupa di ascoltare la blockchain.
* Utilizzando il nostro script di esempio ethers.js, vi concentrerete sull'indirizzo del contratto USDC. Naturalmente, è possibile convertirlo in altri esempi ethers.js utilizzando altri indirizzi di contratto. Inoltre, la funzione "getTransfer" si basa sull'endpoint "WebSocketProvider" della libreria ethers.js. Utilizzando questo endpoint, è possibile definire il provider di nodi che si desidera utilizzare. Per far sì che ciò funzioni, è necessario ottenere anche la chiave di tale provider, che è un aspetto importante dell'utilizzo di ethers.js. L'esempio di codice che segue si concentra su Alchemy. Tuttavia, si dovrebbe utilizzare un provider di nodi che supporti la catena o le catene su cui ci si vuole concentrare.
* Oltre all'indirizzo del contratto e al provider, la funzione "getTransfer" accetta anche un ABI. Infine, è necessario impostare un ascoltatore di "transfer". Quest'ultimo registrerà anche i dettagli relativi alla catena.

const ethers = require("ethers");

const ABI = require("./abi.json");

require("dotenv").config();

async function getTransfer(){

const usdcAddress = "0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48"; ///USDC Contract

const provider = new ethers.providers.WebSocketProvider(

`wss://eth-mainnet.g.alchemy.com/v2/${process.env.ALCHEMY\_KEY}`

);

const contract = new ethers.Contract(usdcAddress, ABI, provider);

contract.on("Transfer", (from, to, value, event)=>{

let transferEvent ={

from: from,

to: to,

value: value,

eventData: event,

}

console.log(JSON.stringify(transferEvent, null, 4))

})

}

getTransfer()

La lettura del bilancio di un particolare account avviene ad esempio come segue:

const { ethers } = require("ethers");

require('dotenv').config()

//we take it from https://app.infura.io/dashboard/ethereum/9f904279fdbb4f5e881c41b51bad948d/settings/endpoints

const provider = new ethers.providers.JsonRpcProvider(`https://mainnet.infura.io/v3/${process.env.INFURA\_ID}`)

//rich contract from EtherScan

const address = '0x73BCEb1Cd57C711feaC4224D062b0F6ff338501e'

const main = async () => {

    const balance = await provider.getBalance(address)

    console.log('Balance: ', balance.toString())

}

main()

La lettura degli smart contract, basandosi su una ABI dello standard ERC-20 che permette la lettura delle funzioni stabilite dallo stesso standard appare come segue:

const { ethers } = require("ethers");

require('dotenv').config()

//we take it from https://app.infura.io/dashboard/ethereum/9f904279fdbb4f5e881c41b51bad948d/settings/endpoints

const provider = new ethers.providers.JsonRpcProvider(`https://mainnet.infura.io/v3/${process.env.INFURA\_ID}`)

//rich contract from EtherScan

const address = '0x6B175474E89094C44Da98b954EedeAC495271d0F' // DAI (which is a stablecoin) Contract

const ERC\_20\_ABI = [

    // Read-Only Functions

    "function name() view returns (string)",

    "function symbol() view returns (string)",

    "function decimals() view returns (uint)",

    "function totalSupply() view returns (uint)",

    "function balanceOf(address) view returns (uint)",

    "function allowance(address, address) view returns (uint)",

    // Write Functions

    "function transfer(address, uint) returns (bool)",

    "function approve(address, uint) returns (bool)",

    "function transferFrom(address, address, uint) returns (bool)",

]

const contract = new ethers.Contract(address, ERC\_20\_ABI, provider)

const main = async () => {

    const name = await contract.name()

    const symbol = await contract.symbol()

    const decimals = await contract.decimals()

    const totalSupply = await contract.totalSupply()

    console.log('Contract Address: ', address)

    console.log('Name: ', name)

    console.log('Symbol: ', symbol)

    console.log('Decimals: ', decimals.toString())

    console.log('Total Supply: ', totalSupply.toString())

    const balance = await contract.balanceOf('0x73BCEb1Cd57C711feaC4224D062b0F6ff338501e')

    console.log('Balance: ', balance.toString())

    console.log(`Balance Formatted: ${ethers.utils.formatEther(balance)}\n`)

}

main()

La creazione di una chiave privata, con annesso completamento base di una transazione è come segue:

const { ethers } = require("ethers");

require('dotenv').config()

//we take it from https://app.infura.io/dashboard/ethereum/9f904279fdbb4f5e881c41b51bad948d/settings/endpoints

const provider = new ethers.providers.JsonRpcProvider(`https://mainnet.infura.io/v3/${process.env.INFURA\_ID}`)

//const account = ethers.Wallet.createRandom() //create a rondom one

//need to have some ether in the account, using Sepolia since it's the only one that receives ethers on the testnet from Chainlink,

//the others are deprecated

const account\_sender = new ethers.Wallet(process.env.SENDER, provider)

const account\_receiver = new ethers.Wallet(process.env.RECEIVER, provider)

//from advanced option on MetaMask, we get the private key

const privateKey = process.env.PRIVATE\_KEY

//we create a wallet from the private key

const wallet = new ethers.Wallet(privateKey, provider)

const main = async () => {

    const balance\_sender = await wallet.getBalance(account\_sender)

    console.log("Balance before transaction of sender: ", ethers.utils.formatEther(balance\_sender))

    const balance\_receiver = await wallet.getBalance(account\_receiver)

    console.log("Balance before transaction of receiver: ", ethers.utils.formatEther(balance\_receiver))

    const tx = await wallet.sendTransaction({

        to: account\_receiver.address,

        value: ethers.utils.parseEther("0.01")

    })

    console.log("Transaction hash: ", tx.hash)

    const receipt = await tx.wait()

    console.log("Transaction receipt: ", receipt)

    const balance\_sender\_after = await wallet.getBalance(account\_sender)

    console.log("Balance after transaction of sender: ", ethers.utils.formatEther(balance\_sender\_after))

    const balance\_receiver\_after = await wallet.getBalance(account\_receiver)

    console.log("Balance after transaction of receiver: ", ethers.utils.formatEther(balance\_receiver\_after))

}

main()

In questo caso, invece, abbiamo i dettagli di una transazione completa di tutti i dettagli utili:

const { ethers } = require("ethers");

require('dotenv').config()

//we take it from https://app.infura.io/dashboard/ethereum/9f904279fdbb4f5e881c41b51bad948d/settings/endpoints

const provider = new ethers.providers.JsonRpcProvider(`https://mainnet.infura.io/v3/${process.env.INFURA\_ID}`)

//const account = ethers.Wallet.createRandom() //create a rondom one

//need to have some ether in the account, using Sepolia since it's the only one that receives ethers on the testnet from Chainlink,

//the others are deprecated

const account\_sender = new ethers.Wallet(process.env.SENDER, provider)

const account\_receiver = new ethers.Wallet(process.env.RECEIVER, provider)

//from advanced option on MetaMask, we get the private key

const privateKey = process.env.PRIVATE\_KEY

//we create a wallet from the private key

const wallet = new ethers.Wallet(privateKey, provider)

const ERC\_20\_ABI = [

    // Some details about the token

    "function name() view returns (string)",

    "function symbol() view returns (string)",

    "function decimals() view returns (uint8)",

    "function totalSupply() view returns (uint256)",

    // Get the account balance

    "function balanceOf(address) view returns (uint256)",

    // Send some of your tokens to someone else

    "function transfer(address to, uint amount)",

    // An event triggered whenever anyone transfers to someone else

    "event Transfer(address indexed from, address indexed to, uint amount)"

]

const contract = new ethers.Contract(process.env.CONTRACT\_ADDRESS, ERC\_20\_ABI, provider)

const main = async () => {

    const name = await contract.name()

    const symbol = await contract.symbol()

    const decimals = await contract.decimals()

    const totalSupply = await contract.totalSupply()

    const balance = await wallet.getBalance(account\_sender)

    console.log("Name: ", name)

    console.log("Symbol: ", symbol)

    console.log("Decimals: ", decimals)

    console.log("Total supply: ", totalSupply.toString())

    console.log("Balance of sender: ", balance.toString())

    const tx = await contractWithWallet.transfer(account\_receiver.address, ethers.utils.parseEther("0.01"))

    console.log("Transaction hash: ", tx.hash)

    const receipt = await tx.wait()

    console.log("Transaction receipt: ", receipt)

    const balance\_sender\_after = await wallet.getBalance(account\_sender)

    console.log("Balance after transaction of sender: ", balance\_sender\_after.toString())

    const balance\_receiver\_after = await wallet.getBalance(account\_receiver)

    console.log("Balance after transaction of receiver: ", balance\_receiver\_after.toString())

}

main()

Ogni dettaglio della transazioni eseguite rimane presente su EtherScan, accessibile anche tramite MetaMask. Il flusso completo di trasferimento di un contratto, completo di filtraggio blocchi e successiva approvazione segue:

const { ethers } = require("ethers");

require('dotenv').config()

//we take it from https://app.infura.io/dashboard/ethereum/9f904279fdbb4f5e881c41b51bad948d/settings/endpoints

const provider = new ethers.providers.JsonRpcProvider(`https://mainnet.infura.io/v3/${process.env.INFURA\_ID}`)

const ERC\_20\_ABI=[

    // Read-Only Functions

    "function name() view returns (string)",

    "function symbol() view returns (string)",

    "function decimals() view returns (uint)",

    "function totalSupply() view returns (uint)",

    "function balanceOf(address) view returns (uint)",

    "function allowance(address, address) view returns (uint)",

    // Write Functions

    "function transfer(address, uint) returns (bool)",

    "function approve(address, uint) returns (bool)",

    "function transferFrom(address, address, uint) returns (bool)",

    // Events - These are emitted when state changes

    "event Transfer(address indexed from, address indexed to, uint value)",

    "event Approval(address indexed owner, address indexed spender, uint value)"

]

const address = '0x6B175474E89094C44Da98b954EedeAC495271d0F' // DAI Contract

const contract = new ethers.Contract(address, ERC20\_ABI, provider)

const main = async () => {

    const block = await provider.getBlockNumber()

    // Filter for Transfer events to and from an address

    const transferFilter = contract.filters.Transfer(null, '0x73BCEb1Cd57C711feaC4224D062b0F6ff338501e') // here we can put the address we want to filter

    const transferEvents = await contract.queryFilter(transferFilter, block - 1000, block) // we can also specify the block range we want to filter

    console.log('Transfer Events: ', transferEvents)

    // Filter for Approval events to and from an address

    const approvalFilter = contract.filters.Approval('0x73BCEb1Cd57C711feaC4224D062b0F6ff338501e', null)

    const approvalEvents = await contract.queryFilter(approvalFilter)

    console.log('Approval Events: ', approvalEvents)

}

main()

Qui di seguito, i dettagli dei singoli blocchi:

const { ethers } = require("ethers");

require('dotenv').config()

//we take it from https://app.infura.io/dashboard/ethereum/9f904279fdbb4f5e881c41b51bad948d/settings/endpoints

const provider = new ethers.providers.JsonRpcProvider(`https://mainnet.infura.io/v3/${process.env.INFURA\_ID}`)

const main = async () => {

    const block = await provider.getBlock(1000000)

    console.log('Block: ', block)

    const blockNumber = await provider.getBlockNumber()

    console.log('Block number: ', blockNumber)

    const blockWithTransactions = await provider.getBlockWithTransactions(1000000)

    console.log('Block with transactions: ', blockWithTransactions)

}

main()

### web3.js

Tutta la sezione ha come riferimento di massima: <https://www.dappuniversity.com/articles/web3-js-intro>

Lo sviluppo di applicazioni blockchain con Ethereum presenta diversi aspetti:

* Sviluppo di contratti intelligenti - scrittura di codice che viene distribuito sulla blockchain con il linguaggio di programmazione Solidity.
* Sviluppo di siti web o client che interagiscono con la blockchain - scrittura di codice che legge e scrive dati dalla blockchain con gli smart contract.

Web3.js consente di adempiere alla seconda responsabilità: sviluppare client che interagiscono con la blockchain Ethereum. Si tratta di una raccolta di librerie che consentono di eseguire azioni come l'invio di Ether da un conto a un altro, la lettura e la scrittura di dati da contratti intelligenti, la creazione di contratti intelligenti e molto altro ancora.

* Web3.js dialoga con la Blockchain di Ethereum con il protocollo JSON RPC, che sta per "Remote Procedure Call". Ethereum è una rete peer-to-peer di nodi che memorizza una copia di tutti i dati e del codice sulla blockchain. Web3.js ci permette di fare richieste a un singolo nodo Ethereum con JSON RPC per leggere e scrivere dati sulla rete. È un po' come usare jQuery con un'API JSON per leggere e scrivere dati su un server web.
* Dipendenze

Ci sono alcune dipendenze che vi aiuteranno a iniziare a sviluppare con Web3.js.

* Gestore di pacchetti Node (NPM)

La prima dipendenza di cui abbiamo bisogno è Node Package Manager, o NPM, che viene fornito con Node.js. Per verificare se Node è già installato, basta andare sul proprio terminale e digitare

$ node -v

* Libreria Web3.js

È possibile installare la libreria Web3.js con NPM nel terminale in questo modo:

$ npm install web3

* URL RPC di Infura

Per connettersi a un nodo Ethereum con JSON RPC sulla rete principale, è necessario accedere a un nodo Ethereum. Ci sono alcuni modi per farlo. Ad esempio, si potrebbe gestire il proprio nodo Ethereum con Geth o Parity. Ma questo richiede di scaricare molti dati dalla blockchain e di mantenerli sincronizzati. Questo è un enorme mal di testa se avete mai provato a farlo prima.

Per comodità, è possibile utilizzare Infura per accedere a un nodo Ethereum senza doverne gestire uno. Infura è un servizio che fornisce gratuitamente un nodo Ethereum remoto. Tutto quello che dovete fare è iscrivervi e ottenere una chiave API e l'URL RPC per la rete a cui volete connettervi.

Una volta effettuata l'iscrizione, l'URL RPC di Infura dovrebbe essere simile a questo:

<https://mainnet.infura.io/YOUR_INFURA_API_KEY>

* Controllare i saldi dei conti

Ora che tutte le dipendenze sono installate, si può iniziare a sviluppare con Web3.js! Per prima cosa, si dovrebbe avviare la console di Node nel terminale, come segue:

$ node

All'interno della console di Node, è possibile richiedere Web3.js in questo modo:

const Web3 = require('web3')

Ora si ha accesso a una variabile in cui è possibile creare una nuova connessione Web3! Prima di generare una connessione Web3, dobbiamo prima assegnare l'URL di Infura a una variabile come questa:

const rpcURL = "https://mainnet.infura.io/YOUR\_INFURA\_API\_KEY"

Assicurarsi di sostituire YOUR\_INFURA\_API\_KEY con la chiave API Infura ottenuta in precedenza. Ora è possibile istanziare una connessione Web3 in questo modo:

const web3 = new Web3(rpcURL)

Ora avete una connessione Web3 attiva che vi permetterà di parlare con la rete principale di Ethereum! Utilizziamo questa connessione per controllare il saldo del conto: 0x90e63c3d53E0Ea496845b7a03ec7548B70014A91. Possiamo vedere quanto Ether detiene questo conto controllando il suo saldo con web3.eth.getBalance().

Per prima cosa, assegniamo l'indirizzo a una variabile:

const account = "0x90e63c3d53E0Ea496845b7a03ec7548B70014A91"

Ora controlliamo il saldo del conto in questo modo:

web3.eth.getBalance(address, (err, wei) => {

balance = web3.utils.fromWei(wei, 'ether')

})

Lasciate che vi spieghi questo codice. Per prima cosa, si controlla il saldo chiamando web3.eth.getBalance(), che accetta una funzione di callback con due argomenti, un errore e il saldo stesso. Per ora ignoreremo l'argomento dell'errore e faremo riferimento al saldo con l'argomento wei. Ethereum esprime i saldi in Wei, che è la più piccola suddivisione di Ether, un po' come un piccolo penny. Possiamo convertire questo saldo in Ether con web3.utils.fromWei(wei, 'ether').

Riassumendo, avremo il seguente codice:

const Web3 = require('web3')

const rpcURL = '' // Il vostro URL RPC va qui

const web3 = new Web3(rpcURL)

const address = '' // L'indirizzo del vostro account va qui

web3.eth.getBalance(address, (err, wei) => {

balance = web3.utils.fromWei(wei, 'ether')

})

* Leggere I dati degli smart contract

Per leggere i dati dagli smart contract con Web3.js, abbiamo bisogno di due cose:

* una rappresentazione in JavaScript dello smart contract con cui vogliamo interagire
* un modo per chiamare le funzioni dello smart contract durante la lettura dei dati.

Possiamo ottenere una rappresentazione JavaScript di uno smart contract Ethereum con la funzione web3.eth.Contract(). Questa funzione si aspetta due argomenti: uno per l'ABI dello smart contract e uno per l'indirizzo dello smart contract.

L'ABI di uno smart contract sta per "Abstract Binary Interface" (Interfaccia binaria astratta) ed è un array JSON che descrive il funzionamento di uno specifico smart contract. Ecco un esempio di ABI:

const abi = [{"constant":true, "input":[], "name": "mintingFinished", "outputs":[{"name":", "type": "bool"}], "payable":false, "type": "function"},{"constant":true, "input":[], "name": "name", "outputs":[{"name":", "type": "stringa"}], "pagabile":false, "tipo": "funzione"},{"constant":false, "ingressi":[{"nome":"\_spender", "tipo": "indirizzo"},{"nome":"\_valore", "tipo": "uint256"}], "nome": "approvare", "uscite":[], "pagabile":false, "tipo": "funzione"},{"constant": true,"inputs":[],"name":"totalSupply","outputs":[{"name":"","type":"uint256"}],"payable":false,"type":"function"},{"constant":false,"inputs":[{"name":"\_from","type":"address"},{"name":"\_to","type":"address"},{"name": "\_valore", "tipo": "uint256"}], "nome": "transferFrom", "uscite":[], "pagabile":false, "tipo": "function"},{"constant":true, "ingressi":[], "nome": "decimali", "uscite":[{"nome":", "tipo": "uint256"}], "pagabile":false, "tipo": "function"},{"constant":false, "input":[], "name": "unpause", "output":[{"name":"", "type": "bool"}], "payable":false, "type": "function"},{"constant":false, "input":[{"name":"\_to", "type": "address"},{"name":"\_amount", "type": "uint256"}],"name":"mint","outputs":[{"name":"","type":"bool"}],"payable":false,"type":"function"},{"constant":true,"inputs":[],"name":"paused","outputs":[{"name":"","type":"bool"}],"payable":false,"type": "function"},{"constant":true, "input":[{"name":"\_owner", "type": "address"}], "name": "balanceOf", "output":[{"name": "balance", "type": "uint256"}], "payable":false, "type": "function"},{"constant":false, "input":[], "name": "finishMinting", "output":[{"name":"", "type": "bool"}], "payable":false, "type": "function"},{"constant":false, "input":[], "name": "pause", "output":[{"name":"", "type": "bool"}], "payable":false, "type": "function"},{"constant":true, "input": [], "nome": "proprietario", "uscite":[{"nome":"", "tipo": "indirizzo"}], "pagabile":false, "tipo": "funzione"},{"costante":true, "ingressi":[], "nome": "simbolo", "uscite":[{"nome":"", "tipo": "stringa"}], "pagabile":false, "tipo": "funzione"},{"costante": false,"inputs":[{"name":"\_to","type":"address"},{"name":"\_value","type":"uint256"}],"name":"transfer","outputs":[],"payable":false,"type":"function"},{"constant":false,"inputs":[{"name":"\_to","type":"address"},{"name": "\_amount","type":"uint256"},{"name":"\_releaseTime","type":"uint256"}],"name":"mintTimelocked","outputs":[{"name":"","type":"address"}],"payable":false,"type":"function"},{"constant":true,"inputs":[{"name":"\_owner","type": "indirizzo"},{"nome":"\_spendente", "tipo": "indirizzo"}], "nome": "indennità", "uscite":[{"nome": "rimanente", "tipo": "uint256"}], "pagabile":false, "tipo": "funzione"},{"costante":false, "ingressi":[{"nome": "nuovoProprietario", "tipo": "indirizzo"}], "nome": "trasferimentoProprietà", "uscite":[], "pagabile":false, "tipo": "funzione"},{"anonymous":false, "input":[{"indexed":true, "name": "to", "type": "address"},{"indexed":false, "name": "value", "type": "uint256"}], "name": "Menta", "tipo": "evento"},{"anonymous":false, "input":[], "name": "MentaFinita", "type": "event"},{"anonymous":false, "input":[], "name": "Pausa", "type": "event"},{"anonymous":false, "input":[], "name": "Unpause", "type": "evento"},{"anonymous":false, "input":[{"indexed":true, "name": "owner", "type": "address"},{"indexed":true, "name": "spender", "type": "address"},{"indexed":false, "name": "value", "type": "uint256"}], "name": "Approval", "type": "evento"},{"anonymous":false, "input":[{"indexed":true, "name": "from", "type": "address"},{"indexed":true, "name": "to", "type": "address"},{"indexed":false, "name": "value", "type": "uint256"}], "name": "Transfer", "type": "event"}].

È un array ininterrotto molto lungo. Questo esempio è l'ABI per il token OmiseGo (OMG), che implementa lo standard ERC-20 (se non conoscete questo standard, potete guardare questo video). Potete trovare maggiori dettagli su questo token, compresi il suo abi e il suo indirizzo su Etherscan. Utilizzeremo questo ABI per il resto dell'esempio.

Già che ci siamo, procederò a memorizzare l'indirizzo del token OMG dalla rete principale di Ethereum:

const address = "0xd26114cd6EE289AccF82350c8d8487fedB8A0C07"

Ora che abbiamo assegnato entrambi i valori, possiamo creare una rappresentazione JavaScript completa dello smart contract OMG token in questo modo:

const contract = new web3.eth.Contract(abi, address)

Ora che la prima parte di questa lezione è stata completata, è necessario adempiere alla seconda parte: leggere i dati dallo smart contract chiamando le sue funzioni. Tutte le funzioni dello smart contract sono elencate nello spazio dei nomi contract.methods all'interno del contratto Web3 assegnato. Per esempio, possiamo chiamare contract.methods.myFunction() se il contratto implementa myFunction().

Ottimo! Quindi, in teoria, possiamo chiamare qualsiasi funzione implementata dal contratto smart. Ma come facciamo a sapere quali funzioni implementa? Ad esempio, potremmo registrare contract.methods nella console e vedere cosa viene restituito (potete vedere come lo faccio nel video qui sopra). Tuttavia, poiché questo smart contract implementa lo standard ERC-20, sappiamo che implementa diverse funzioni come totalSupply(), name(), symbol() e balanceOf(). Possiamo leggere ciascuno di questi valori singolarmente, in questo modo che segue.

In primo luogo, l'offerta totale di tutti i token OMG esistenti:

contract.methods.totalSupply().call((err, result) => { console.log(result) })

// > 140245398

In secondo luogo, il nome del token OMG:

contract.methods.name().call((err, result) => { console.log(result) })

// > Token OMG

Terzo, il simbolo del token OMG:

contract.methods.symbol().call((err, result) => { console.log(result) })

// > OMG

Infine, possiamo controllare il saldo di un determinato conto. Ho cercato un titolare di OMG ricco su Etherscan e ho trovato questo indirizzo 0xd26114cd6EE289AccF82350c8d8487fedB8A0C07. Possiamo controllare il saldo di questo conto in questo modo:

contract.methods.balanceOf('0xd26114cd6EE289AccF82350c8d8487fedB8A0C07').call((err, result) => { console.log(result) })

// > Un numero molto grande...

E questo è tutto! Ecco quanto è facile leggere i dati dagli smart contract con Web3.js.

* Nelle transazioni Ethereum

Oltre all'apprendimento di Web3.js, lo scopo di questa lezione è quello di aiutarvi a comprendere le basi del funzionamento delle transazioni sulla blockchain di Ethereum. Ogni volta che si crea una transazione, si scrivono dati sulla blockchain e si aggiorna il suo stato. Ci sono diversi modi per farlo, come l'invio di Ether da un conto a un altro, la chiamata di una funzione dello smart contract che scrive dati e il deploy di uno smart contract sulla blockchain. Possiamo comprendere meglio questi concetti eseguendo queste azioni con la libreria Web3.js e osservando come funziona ogni fase.

Per trasmettere le transazioni alla rete, dobbiamo prima firmarle. Per farlo, utilizzerò una libreria JavaScript aggiuntiva, chiamata ethereumjs-tx. È possibile installare questa dipendenza dalla riga di comando in questo modo:

$ npm install ethereumjs-tx

Il motivo per cui utilizzeremo questa libreria è che vogliamo firmare tutte le transazioni localmente. Se gestissimo il nostro nodo Ethereum in locale, potremmo sbloccare un account memorizzato in loco e firmare tutte le nostre transazioni in loco. Se così fosse, non avremmo necessariamente bisogno di usare questa libreria. Tuttavia, in questo tutorial stiamo utilizzando un nodo remoto ospitato da Infura. Sebbene Infura sia un servizio affidabile, vogliamo comunque firmare le transazioni localmente piuttosto che dare al nodo remoto la gestione delle nostre chiavi private.

Questo è esattamente ciò che faremo in questa lezione. Vi mostrerò come creare la transazione grezza, firmarla, quindi inviarla e trasmetterla alla rete! Per fare questo, creerò un semplice file app.js per eseguire il codice di questa lezione, invece di fare tutto nella console.

All'interno del file app.js, per prima cosa richiederemo la libreria appena installata in questo modo:

var Tx = require('ethereumjs-tx')

Quindi, configureremo una connessione Web3 come abbiamo fatto nelle lezioni precedenti:

const Web3 = require('web3')

const web3 = new Web3('https://ropsten.infura.io/YOUR\_INFURA\_API\_KEY')

Notate che stiamo usando la rete di test di Ropsten, che è diversa dalla rete principale di Ethereum che abbiamo usato nella lezione precedente. Vogliamo usare una rete di prova perché tutte le transazioni costano gas sotto forma di Ether. Possiamo utilizzare Ether falsi sulla rete di prova di Ropsten senza preoccuparci di spendere denaro. È possibile ottenere Ether falso da un rubinetto sulla rete di test Ropsten con un rubinetto. Ecco due faucet che si possono utilizzare:

* <http://faucet.ropsten.be:3001/>
* <https://faucet.metamask.io/>

In questa lezione creeremo una transazione che invia falsi Ether da un conto a un altro. Per farlo, avremo bisogno di due conti e delle loro chiavi private. È possibile creare nuovi account con Web3.js in questo modo:

web3.eth.accounts.create()

// > {

// indirizzo: "0xb8CE9ab6943e0eCED004cDe8e3bBed6568B2Fa01",

// privateKey: "0x348ce564d427a3311b6536bbcff9390d69395b06ed6c486954e971d960fe8709",

// signTransaction: function(tx){...},

// sign: function(data){...},

// encrypt: function(password){...}

// }

Una volta creati entrambi i conti, assicuratevi di caricarli con Ether falso da un rubinetto. Ora, li assegneremo alle variabili del nostro script in questo modo:

const account1 = '0xb8CE9ab6943e0eCED004cDe8e3bed6568B2Fa01'

const account2 = '0xb8CE9ab6943e0eCED004cDe8e3bBed6568B2Fa02'

Assicurarsi di utilizzare gli account generati, poiché questi account non funzioneranno per questa lezione. Ora, salviamo le chiavi private nell'ambiente in questo modo:

export PRIVATE\_KEY\_1='la vostra chiave privata 1'

export PRIVATE\_KEY\_1='la tua chiave privata 2 qui'

Vogliamo salvare queste chiavi private nell'ambiente, in modo da evitare di inserirle nel nostro file. È una cattiva pratica esporre le chiavi private in questo modo. Che cosa succederebbe se per sbaglio le caricassimo nei sorgenti di un progetto reale? Qualcuno potrebbe rubare il nostro Ether! Ora vogliamo leggere queste chiavi private dal nostro ambiente e memorizzarle in variabili. Possiamo farlo con l'oggetto globale process in NodeJS, in questo modo:

const privateKey1 = process.env.PRIVATE\_KEY\_1

const privateKey2 = process.env.PRIVATE\_KEY\_2

Per firmare le transazioni con le chiavi private, dobbiamo convertirle in una stringa di dati binari con un Buffer, un modulo disponibile a livello globale in NodeJS. Possiamo farlo in questo modo:

const privateKey1 = Buffer.from(process.env.PRIVATE\_KEY\_1)

const privateKey1 = Buffer.from(process.env.PRIVATE\_KEY\_2)

Bene, ora abbiamo impostato tutte le nostre variabili! So che alcune di queste cose potrebbero essere un po' confuse a questo punto.

A questo punto, vogliamo fare alcune cose:

* Creare un oggetto transazione
* Firmare la transazione
* Trasmettere la transazione alla rete

Possiamo costruire l'oggetto transazione in questo modo:

const txObject = {

nonce: web3.utils.toHex(txCount),

to: account2,

valore: web3.utils.toHex(web3.utils.toWei('0.1', 'ether')),

gasLimit: web3.utils.toHex(21000),

gasPrice: web3.utils.toHex(web3.utils.toWei('10', 'gwei'))

}

Lasciate che vi spieghi questo codice. Stiamo costruendo un oggetto che contiene tutti i valori necessari per generare una transazione, come nonce, to, value, gasLimit e gasPrice. Analizziamo ciascuno di questi valori:

* nonce - è il conteggio delle transazioni precedenti per il conto in questione. Assegneremo il valore di questa variabile tra poco. Dobbiamo anche convertire questo valore in esadecimale. Possiamo farlo con l'utility Web3.js web3.utils.toHex()
* to - il conto a cui stiamo inviando Ether.
* value - la quantità di Ether che vogliamo inviare. Questo valore deve essere espresso in Wei e convertito in esadecimale. Possiamo convertire il valore in Wei con l'utilità web3.js web3.utils.toWei().
* gasLimit - è la quantità massima di gas consumata dalla transazione. Una transazione di base come questa costa sempre 21000 unità di gas, quindi useremo questo valore.
* gasPrice - è l'importo che vogliamo pagare per ogni unità di gas. Qui utilizzeremo 10 Gwei.

Si noti che non c'è un campo from in questo oggetto transazione. Questo verrà dedotto quando firmeremo la transazione con la chiave privata di account1.

Ora assegniamo il valore della variabile nonce. Possiamo ottenere il nonce della transazione con la funzione web3.eth.getTransactionCount(). Avvolgeremo tutto il nostro codice all'interno di una funzione di callback come questa:

web3.eth.getTransactionCount(account1, (err, txCount) => {

const txObject = {

nonce: web3.utils.toHex(txCount),

to: account2,

valore: web3.utils.toHex(web3.utils.toWei('0.1', ‘ether’)),

gasLimit: web3.utils.toHex(21000),

gasPrice: web3.utils.toHex(web3.utils.toWei('10', 'gwei'))

}

})

Ed ecco l'oggetto transazione completato! Abbiamo completato il passo 1. :) Ora dobbiamo passare al passo 2, in cui firmiamo la transazione. Possiamo farlo in questo modo:

const tx = new Tx(txObject)

tx.sign(privateKey1)

const serializedTx = tx.serialize()

const raw = '0x' + serializedTx.toString('hex')

Qui usiamo la libreria etheremjs-tx per creare un nuovo oggetto Tx. Usiamo questa libreria anche per firmare la transazione con privateKey1. Quindi, serializziamo la transazione e la convertiamo in una stringa esadecimale, in modo da poterla passare a Web3.

Infine, inviamo la transazione firmata e serializzata alla rete di test con la funzione web3.eth.sendSignedTransaction() in questo modo:

web3.eth.sendSignedTransaction(raw, (err, txHash) => {

console.log('txHash:', txHash)

})

Ed ecco fatto! Questo è il passo finale di questa lezione, che invia la transazione e la trasmette alla rete. A questo punto, il file app.js completato dovrebbe avere questo aspetto:

var Tx = require('ethereumjs-tx')

const Web3 = require('web3')

const web3 = new Web3('https://ropsten.infura.io/YOUR\_INFURA\_API\_KEY')

const account1 = '' // L'indirizzo del vostro conto 1

const account2 = '' // L'indirizzo del vostro conto 2

const privateKey1 = Buffer.from('YOUR\_PRIVATE\_KEY\_1', 'hex')

const privateKey2 = Buffer.from('YOUR\_PRIVATE\_KEY\_2', 'hex')

web3.eth.getTransactionCount(account1, (err, txCount) => {

// Crea la transazione

const txObject = {

nonce: web3.utils.toHex(txCount),

to: account2,

valore: web3.utils.toHex(web3.utils.toWei('0.1', 'ether')),

gasLimit: web3.utils.toHex(21000),

gasPrice: web3.utils.toHex(web3.utils.toWei('10', 'gwei'))

}

// Firmare la transazione

const tx = new Tx(txObject)

tx.sign(privateKey1)

const serializedTx = tx.serialize()

const raw = '0x' + serializedTx.toString('hex')

// Trasmettere la transazione

web3.eth.sendSignedTransaction(raw, (err, txHash) => {

console.log('txHash:', txHash)

// Ora controllate etherscan per vedere la transazione!

})

})

* Deploy dei contratti a Web3

Esistono diversi modi per distribuire i contratti intelligenti sulla Blockchain di Ethereum. Ci sono anche diversi modi per distribuirli all'interno di Web3.js stesso. Come nella lezione precedente di questa serie, vi mostrerò un metodo che vi aiuterà a capire meglio cosa succede quando uno smart contract viene distribuito su Ethereum Blockchain. Questo esempio è stato progettato per suddividere il deployment in ogni fase del processo.

Questa lezione utilizzerà lo stesso file app.js che abbiamo usato nella lezione precedente. Lo imposteremo in questo modo:

Per seguire l'esercitazione, si consiglia di leggere questo codice:

var Tx = require('ethereumjs-tx')

const Web3 = require('web3')

const web3 = new Web3('https://ropsten.infura.io/YOUR\_INFURA\_API\_KEY')

const account1 = '' // L'indirizzo del vostro conto 1

const privateKey1 = Buffer.from('YOUR\_PRIVATE\_KEY\_1', 'hex')

Questo esempio di lezione consisterà negli stessi tre passi fondamentali della lezione precedente:

* Creare un oggetto transazione
* Firmare la transazione
* Inviare la transazione

Questi passaggi sono gli stessi perché ogni volta che scriviamo dati sulla blockchain, si tratta sempre degli stessi passaggi di base. Sto cercando di mostrarvi che l'implementazione di un contatto intelligente è in realtà molto simile all'invio di Ether da un conto a un altro, o alla chiamata di una funzione di uno smart contract. Stiamo ancora creando una transazione e la stiamo inviando alla rete. L'unica differenza sono i parametri della transazione.

Procediamo a costruire l'oggetto transazione in questo modo:

const txObject = {

nonce: web3.utils.toHex(txCount),

gasLimit: web3.utils.toHex(1000000), // Aumenta il limite di gas a un importo molto più alto

gasPrice: web3.utils.toHex(web3.utils.toWei('10', 'gwei')),

dati: dati

}

Stiamo costruendo questo oggetto transazione che ha molti degli stessi campi dell'oggetto della lezione precedente, come nonce, gasLimit e gasPrice. Ci sono anche alcune differenze fondamentali. Analizziamo ciascuno di essi:

* nonce - è il conteggio delle transazioni precedenti per il conto in questione. È lo stesso della lezione precedente.
* gasLimit - è la quantità massima di gas consumata dalla transazione. Aumenteremo questo limite perché la distribuzione di contratti intelligenti richiede molto più gas dell'invio di Ether.
* gasPrice - è l'importo che vogliamo pagare per ogni unità di gas. È lo stesso della lezione precedente.
* value - questo parametro è assente in questo esempio perché non stiamo inviando alcun Ether in questa transazione.
* to - questo parametro è assente perché non stiamo inviando questa transazione a un conto particolare. La stiamo invece inviando all'intera rete, perché stiamo distribuendo uno smart contract!
* data - questo sarà il bytecode dello smart contract che vogliamo distribuire. Assegneremo a questa variabile un valore, che spiegherò meglio tra poco.

Parliamo del parametro data. Si tratta della rappresentazione bytecode compilata dello smart contract in esadecimale. Per ottenere questo valore, abbiamo prima bisogno di uno smart contract e poi di compilarlo! Potete usare qualsiasi contratto smart che vi piace, soprattutto perché lo stiamo distribuendo su una rete di prova. Tuttavia, io utilizzerò uno smart contract con token ERC-20 che ho costruito in questo video. Potete seguirmi nel video tutorial Web3.js qui sopra per vedere come compilo questo particolare smart contract ERC-20 con Remix per ottenere questa stringa di dati. Una volta compilato il contratto, si può assegnare il valore dei dati a una variabile come questa:

const data = '0x60806040526040805190810160405280600a81526020017f44…

const txObject = {

nonce: web3.utils.toHex(txCount),

gasLimit: web3.utils.toHex(1000000), // Raise the gas limit to a much higher amount

gasPrice: web3.utils.toHex(web3.utils.toWei('10', 'gwei')),

data: data

}

const tx = new Tx(txObject)

tx.sign(privateKey1)

const serializedTx = tx.serialize()

const raw = '0x' + serializedTx.toString('hex')

web3.eth.sendSignedTransaction(raw, (err, txHash) => {

console.log('err:', err, 'txHash:', txHash)

// Use this txHash to find the contract on Etherscan!

})

})

* Chiamare funzioni degli smart contract

Questa lezione utilizzerà molti degli stessi passaggi di base delle lezioni precedenti perché, come le lezioni precedenti, è stata pensata per mostrare tutti i passaggi di base necessari per creare transazioni sulla Blockchain di Ethereum. Utilizzeremo la stessa configurazione di base con un file app.js che avrà questo aspetto:

const Web3 = require('web3')

const web3 = new Web3('https://ropsten.infura.io/YOUR\_INFURA\_API\_KEY')

const account1 = '' // L'indirizzo del vostro account 1

const account2 = '' // L'indirizzo del vostro conto 2

const privateKey1 = Buffer.from('YOUR\_PRIVATE\_KEY\_1', 'hex')

const privateKey2 = Buffer.from('YOUR\_PRIVATE\_KEY\_2', 'hex')

Creeremo anche un oggetto transazione, proprio come questo:

const txObject = {

nonce: web3.utils.toHex(txCount),

gasLimit: web3.utils.toHex(800000),

gasPrice: web3.utils.toHex(web3.utils.toWei('10', 'gwei')),

a: contractAddress,

dati: dati

}

Se avete seguito le lezioni precedenti, molti di questi valori dovrebbero esservi familiari. Prendiamo nota di alcuni cambiamenti.

* to - Questo parametro sarà l'indirizzo del contratto distribuito. Otterremo questo valore e lo assegneremo a breve.
* data - sarà la rappresentazione esadecimale della funzione che vogliamo chiamare sullo smart contract. Anche questo valore sarà assegnato momentaneamente.

Per compilare questi valori, dovremo ottenere l'ABI del contratto smart per questo token ERC-20. Potete seguirmi nel video qui sopra mentre ottengo l'ABI da Remix. Dovrò anche ottenere l'indirizzo dello smart contract da Etherscan (questo era disponibile quando abbiamo distribuito lo smart contract nell'ultima lezione). Ora che abbiamo entrambe le cose, possiamo creare una rappresentazione in JavaScript dello smart contract con Web3.js in questo modo:

const contractAddress = '0xd03696B53924972b9903eB17Ac5033928Be7D3Bc'

const contractABI = [{"constant":true, "inputs":[], "name": "name", "outputs":[{"name":", "type": "string"}], "payable":false, "stateMutability": "view","type":"function"},{"constant":false,"inputs":[{"name":"\_spender","type":"address"},{"name":"\_value","type":"uint256"}],"name": "approva", "uscite":[{"nome": "successo", "tipo": "bool"}], "pagabile":false, "statoMutabilità": "non pagabile", "tipo": "funzione"},{"costante":true, "ingressi": [], "nome": "totalSupply", "output":[{"nome":", "tipo": "uint256"}], "payable":false, "stateMutability": "view", "type": "function"},{"constant": false,"inputs":[{"name":"\_from","type":"address"},{"name":"\_to","type":"address"},{"name":"\_value","type":"uint256"}],"name":"transferFrom","outputs": [{"name": "success", "type": "bool"}], "payable":false, "stateMutability": "nonpayable", "type": "function"},{"constant":true, "input": [], "nome": "standard", "uscite":[{"nome":"", "tipo": "stringa"}], "pagabile":false, "mutabilità di stato": "vista", "tipo": "funzione"},{"costante": true, "input":[{"name":"", "type": "address"}], "name": "balanceOf", "output":[{"name":"", "type": "uint256"}], "payable":false, "stateMutability": "view", "type": "function"},{"constant":true, "input":[], "name": "symbol", "output":[{"name":"", "type": "string"}], "payable":false, "stateMutability": "view","type":"function"},{"constant":false,"inputs":[{"name":"\_to","type":"address"},{"name":"\_value","type":"uint256"}],"name": "trasferimento", "uscite":[{"nome": "successo", "tipo": "bool"}], "pagabile":false, "statoMutabilità": "non pagabile", "tipo": "funzione"},{"costante": true,"inputs":[{"name":"","type":"address"},{"name":"","type":"address"}],"name":"allowance","outputs":[{"name":"","type":"uint256"}],"payable": false, "stateMutability": "view", "type": "function"},{"input":[], "payable":false, "stateMutability": "nonpayable", "type": "constructor"},{"anonymous": false, "input":[{"indexed":true, "name":"\_from", "type": "address"},{"indexed":true, "name":"\_to", "type": "address"},{"indexed":false, "name": "\_valore", "tipo": "uint256"}], "nome": "Trasferimento", "tipo": "evento"},{"anonymous":false, "input":[{"indexed":true, "name":"\_owner", "type": "address"},{"indexed":true,"name":"\_spender","type":"address"},{"indexed":false,"name":"\_value","type":"uint256"}],"name":"Approval","type":"event"}]

const contract = new web3.eth.Contract(abi, contractAddress)

Ottimo! Ora abbiamo una rappresentazione JavaScript del contratto distribuito. Ora possiamo compilare il campo dati della transazione convertendo la funzione transfer() del contratto in bytecode (è la funzione che chiameremo su questo smart contract). Possiamo farlo con la funzione Web3.js encodeABI(), disponibile sull'oggetto contratto. L'aspetto è questo:

const data = contract.methods.transfer(account2, 1000).encodeABI()

Ecco fatto! Ecco quanto è facile codificare questa chiamata di funzione per la transazione! Si noti che stiamo trasferendo 1.000 gettoni al conto2. Questo metodo si occupa di codificare anche i parametri della funzione!

Questo è tutto ciò di cui abbiamo bisogno per costruire l'oggetto transazione. Come nelle lezioni precedenti, ora possiamo firmare la transazione e inviarla. Una volta fatto, possiamo registrare i valori dei saldi dei conti per vedere che la funzione dello smart contract è stata chiamata e che il trasferimento dei token è stato completato.

* Eventi degli smart contract con Web3.js

Gli smart contract di Ethereum hanno la capacità di emettere eventi che indicano che è successo qualcosa nell'esecuzione del codice dello smart contract. I consumatori hanno la possibilità di sottoscrivere questi eventi e Web3.js ci fornirà questa funzionalità. Questo è esattamente ciò che tratteremo in questa lezione.

Continueremo a usare uno smart contract ERC-20 come punto di riferimento per questa esercitazione, perché questo standard specifica che lo smart contract deve emettere un evento Transfer ogni volta che un token ERC-20 viene trasferito. Ci collegheremo alla rete principale di Ethereum per sottoscrivere l'evento Transfer per il token ERC-20 di OmiseGo

Procediamo con la configurazione del file app.js, come abbiamo fatto nelle lezioni precedenti. Questa volta, ci collegheremo alla rete principale di Ethereum. Incolliamo l'ABI e l'indirizzo dello smart contract OmiseGo, che possono essere ottenuti da Etherscan (guardate il video qui sopra per le istruzioni). Una volta ottenute queste due informazioni, possiamo creare una rappresentazione JavaScript dello smart contract con Web3.js e assegnarla a una variabile

* Ispezione dei blocchi con Web3

L'ispezione dei blocchi è spesso utile per analizzare la storia della Blockchain di Ethereum. Web3.js ha molte funzionalità che ci aiutano a fare proprio questo. Ad esempio, potremmo costruire qualcosa che assomigli a questa funzione di cronologia dei blocchi su Etherscan:

Prepariamo un file app.js per iniziare a utilizzare alcune delle funzionalità fornite da Web3.js. Questa configurazione sarà molto più semplice rispetto alle lezioni precedenti. Ci collegheremo alla rete principale per ispezionare i blocchi:

const Web3 = require('web3')

const web3 = new Web3('https://mainnet.infura.io/YOUR\_INFURA\_API\_KEY')

Per prima cosa, possiamo ottenere il numero dell'ultimo blocco in questo modo:

web3.eth.getBlockNumber().then(console.log)

Possiamo anche ottenere tutti i dati dell'ultimo blocco in questo modo:

web3.eth.getBlock('latest').then(console.log)

Se volessimo creare una funzione di cronologia dei blocchi come quella di Etherscan illustrata sopra, dovremmo ottenere un elenco dei blocchi più recenti nella catena. Possiamo farlo recuperando il blocco più recente e contando all'indietro fino agli ultimi 10 blocchi della catena. Possiamo farlo con un ciclo for come questo:

web3.eth.getBlockNumber().then((latest) => {

for (let i = 0; i < 10; i++) {

web3.eth.getBlock(latest - i).then(console.log)

}

})

Web3.js ha un'altra bella funzione che consente di ispezionare le transazioni contenute in un blocco specifico. Possiamo farlo in questo modo:

const hash = '0x66b3fd79a49dafe44507763e9b6739aa0810de2c15590ac22b5e2f0a3f502073'

web3.eth.getTransactionFromBlock(hash, 2).then(console.log)

* Web3 Utilities

Colleghiamoci alla rete principale di Ethereum in questo modo:

const Web3 = require('web3')

const web3 = new Web3('https://mainnet.infura.io/YOUR\_INFURA\_API\_KEY')

Per prima cosa, è possibile ottenere il prezzo medio del gas per la rete in questo modo:

web3.eth.getGasPrice().then((result) => {

console.log(web3.utils.fromWei(result, 'ether'))

})

Se avete già sviluppato sulla blockchain, probabilmente avete avuto a che fare con le funzioni di hashing. Web3.js ha molti aiuti integrati per l'uso delle funzioni di hashing. È possibile accedere direttamente alla funzione sha3 in questo modo:

console.log(web3.utils.sha3('Dapp University'))

Oppure come keccack256:

console.log(web3.utils.keccak256('Dapp University'))

Si può anche gestire la (pseudo) casualità generando un esagono casuale di 32 byte come questo:

console.log(web3.utils.randomHex(32))

Vi siete mai trovati a cercare di eseguire un'azione su un array o un oggetto JavaScript e avete avuto bisogno dell'aiuto di una libreria esterna? Fortunatamente, Web3.js viene fornito con la libreria underscoreJS:

const \_ = web3.utils.\_

\_.each({ key1: 'value1', key2: 'value2' }, (value, key) => {

console.log(key)

})

E questo è tutto! Questi sono alcuni suggerimenti e trucchi di fantasia che potete utilizzare con Web3.js. Ecco il codice completo di questa lezione:

const Web3 = require('web3')

const web3 = new Web3('https://mainnet.infura.io/YOUR\_INFURA\_API\_KEY')

// Ottenere il prezzo medio del gas in wei dagli ultimi blocchi di prezzo mediano del gas

web3.eth.getGasPrice().then((result) => {

console.log(web3.utils.fromWei(result, 'ether'))

})

// Utilizzare la funzione di hashing sha256

console.log(web3.utils.sha3('Dapp University'))

// Utilizzare la funzione di hashing keccak256 (alias)

console.log(web3.utils.keccak256('Dapp University'))

// Ottenere un esadecimale casuale

console.log(web3.utils.randomHex(32))

// Ottenere l'accesso alla libreria JS underscore

const \_ = web3.utils.\_

\_.each({ key1: 'value1', key2: 'value2' }, (value, key) => {

console.log(key)

})

## Vulnerabilità di Solidity e degli smart contract

Ci sono molte vulnerabilità che emergono nella creazione degli smart contract; l’intento di questa sezione è di considerarne quante più possibili e immaginare le possibili soluzioni, corredando il tutto con esempi pratici.

Prendiamo ad esempio un codice semplice, al quale aggiungeremo una funzione di impostazione del prezzo:

Immagine che contiene testo

Descrizione generata automaticamenteImmagine che contiene testo

Descrizione generata automaticamente Riferimenti di questi codici ed immagini: <https://www.gofyeo.com/post/vulnerabilities-in-solidity-smart-contracts>

Ora possiamo aggiornare il prezzo in qualsiasi momento, ma questa funzione ha introdotto alcuni problemi:

* Manca la convalida del mittente: chiunque può modificare il prezzo.
* Manca la convalida degli input: se il prezzo è impostato a 0, i token possono essere acquistati gratuitamente.

Per convalidare il mittente, dobbiamo memorizzare l'indirizzo che è autorizzato a eseguire operazioni di amministrazione.

Immagine che contiene testo

Descrizione generata automaticamente

Ora il proprietario sarà impostato sull'indirizzo che ha distribuito il contratto e solo questo indirizzo sarà in grado di modificare il prezzo. Inoltre, abbiamo aggiunto il controllo che il prezzo sia maggiore di 0 sia nel costruttore che nel setter. Si consiglia di eseguire un controllo di correttezza dei valori importanti anche nel costruttore.

La logica successiva che possiamo aggiungere a questo contratto è quella delle commissioni: ogni volta che l'utente acquista un token, il 5% delle entrate deve andare a un indirizzo dedicato.

Immagine che contiene testo

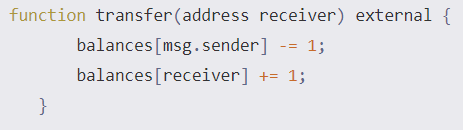
Descrizione generata automaticamente

La matematica potrebbe sembrare corretta: calcoliamo quanto è l'1% e poi lo moltiplichiamo per ottenere il 5%. Purtroppo, la divisione di numeri interi restituisce solo un quoziente e un promemoria andrebbe perso.

Se nel nostro esempio l'importo è 40, allora (40/100)\*5 restituirà 0, anche se il risultato corretto è 2. *Si dovrebbe sempre eseguire la moltiplicazione prima della divisione.*

Inoltre, abbiamo aggiunto una funzione per impostare l'indirizzo di feeCollector, ma il costruttore rimane invariato. *Le* *variabili non inizializzate sono impostate per default a 0*. Ciò significa che per default feeCollector sarebbe address(0) e, a causa della mancata validazione, possiamo impostare manualmente questo valore. *I PF inviati all'indirizzo(0) andrebbero persi.*

Ora gli utenti possono acquistare i token ma non possono utilizzarli. Diamo loro la possibilità di trasferire un token a qualcuno.



La funzione è molto semplice: basta diminuire il saldo del mittente e aggiungere il token all'indirizzo del destinatario. Si può notare che non ci sono controlli per verificare se il mittente ha token nel suo saldo. In questo esempio la versione del compilatore è impostata a >= 0.8.0, dove solidity controlla automaticamente i casi di underflow/overflow. Se si tenta di sottrarre da uno zero, viene generato un errore. *Prima di solidity 0.8.0 era necessario controllare manualmente la presenza di underflow/overflow o utilizzare una libreria speciale come SafeMath.*

*Si ricordi inoltre che la visibilità di default delle funzioni è pubblica e queste dovrebbero essere valutate quando devono essere accessibili all’esterno.*

Aggiungiamo una funzione che trasferisce token a due destinatari:

Immagine che contiene testo

Descrizione generata automaticamente

Il contratto sembra essere completato, ma manca ancora una parte importante. Quando il token viene acquistato, il 95% del prezzo rimarrà nel saldo del contratto, ma non c'è modo di ritirarlo. È importante *assicurarsi che il contratto abbia una funzionalità di prelievo di ETH se ha funzioni di pagamento.*

Immagine che contiene testo

Descrizione generata automaticamente

Come per altri linguaggi, occorre specificare i contratti nell’ordine giusto quando si lavora con l’ereditarietà multipla, sapendo che verrà considerato l’ultimo contratto ereditato.

Quando invece si hanno più variabili con lo stesso nome, si ha il *variable shadowing* come nel codice che segue:

Immagine che contiene testo

Descrizione generata automaticamente

Quando si verifica lo shadowing delle variabili, *entrambe le variabili vengono create in memoria e sono accessibili dal contratto corrispondente*. Nel contratto di esempio, Derived::getValueBase() restituirà 1.

Alcuni problemi comuni qui esaminati:

* Controlla se un valore deve essere modificato dopo la distribuzione;
* Controllare la convalida del mittente;
* Controllare la convalida degli input;
* Eseguire la moltiplicazione prima della divisione;
* Ricordare che le variabili non inizializzate sono 0 per impostazione predefinita;
* Controllare che l'ETH non venga inviato all'indirizzo(0);
* Controllare che vengano gestiti underflow/overflow;
* Verificare che ogni funzione specifichi il livello di visibilità;
* Verificare che le funzioni pubbliche siano accessibili dall'esterno;
* Assicurarsi che il contratto abbia una funzionalità di ritiro dell'ETH se ha funzioni a pagamento;
* Controllare l'ordine di ereditarietà;
* Verificare lo shadowing delle variabili;
* Verificare come vengono utilizzate le funzioni sovrascritte nel contratto di base.

Ulteriori vulnerabilità che si possono considerare:

* Salvare dati riservati non criptati sulla blockchain
  + La blockchain è accessibile a chiunque, il che significa che non c'è assolutamente nulla di riservato; se per errore vi si salvano password (o informazioni simili), ci si trova in grossi guai.
* Soluzione: Non memorizzare mai informazioni riservate su una blockchain, a meno che non vengano crittografate o sottoposte a hash.
* Overflow e underflow di interi (risolto da solidity 0.8)
  + Questa è probabilmente una delle vulnerabilità più facili da capire e da dimenticare allo stesso tempo. Solidity offre diversi tipi di interi in base al valore massimo disponibile: int8 (8 bit, valore massimo 2⁸-1), int16 (16 bit, valore massimo 2¹⁶-1), ...
  + Se si esegue un calcolo che restituisce un risultato più grande del valore massimo o più piccolo di 0, Solidity non lancerà un'eccezione, ma salterà all'altro capo dell'intervallo, ad esempio, per un uint8, 2⁸-1 + 4 = 3...
* Soluzione: Fortunatamente questa vulnerabilità è stata risolta a partire da solidity 0.8. Se si utilizza ancora una versione inferiore di solidity, è possibile utilizzare la libreria SafeMath di OpenZeppelin o verificare da soli la presenza di integer overflow/underflow.
* Valori di ritorno delle chiamate non controllati
  + A un certo punto del vostro codice, potreste invocare una funzione da uno smart contract di terze parti. L'esecuzione potrebbe fallire o restituire un risultato inaspettato.
* Soluzione: Occorre sempre controllare ogni valore ritornato, specie quando si ha a che fare con valori nulli. Dipende sempre dal tipo di funzione e da cosa ritorna.
* Re-entrancy attacks (attacchi di rientranza)
  + Questa è probabilmente la vulnerabilità più nota dell'elenco. Ogni volta che si invoca una funzione di un contratto esterno, bisogna sempre tenere presente che questo contratto potrebbe invocare a sua volta la funzione del proprio contratto (creando una sorta di ciclo di invocazione).
  + Questo può essere potenzialmente pericoloso se, ad esempio, si inviano fondi a un conto esterno (che si dà il caso sia un contratto esterno), ma non si è aggiornato il suo saldo prima di inviarli. Ogni volta che il contratto esterno "rientrerà" nella funzione, riceverà la stessa quantità di fondi. Al termine dell'esecuzione, l'importo inviato sarà probabilmente più volte superiore a quello previsto. Vediamo un esempio di seguito.

Prendiamo questa funzione:

Immagine che contiene testo

Descrizione generata automaticamente

Riferimento di questo codice e dei pezzi successivi: <https://medium.com/coinmonks/protect-your-solidity-smart-contracts-from-reentrancy-attacks-9972c3af7c21>

Tutto ciò di cui un aggressore ha bisogno per sfruttare questa funzione è ottenere una certa quantità di saldo mappata all'indirizzo del proprio smart contract e creare una funzione di fallback che chiami *withdraw*.

Dopo che *msg.sender.call.value(amount)()* trasferisce l'importo corretto, la funzione di fallback dell'attaccante chiama nuovamente withdraw, trasferendo altri fondi prima che *balances[msg.sender] = 0* possa fermare ulteriori trasferimenti. Questa procedura continua fino a quando non rimane più etere o l'esecuzione raggiunge la dimensione massima dello stack.

In genere una funzione vulnerabile effettua una chiamata esterna utilizzando *transfer*, *send* o *call*. Le differenze tra queste funzioni saranno trattate nella sezione dedicata alla prevenzione degli attacchi di rientranza.

Esistono diversi tipi di attacchi di rientranza:

* Attacco di rientranza a funzione singola (Single function reentrancy attack)
  + Questo tipo di attacco è il più semplice e facile da prevenire. Si verifica quando la funzione vulnerabile è la stessa funzione che l'attaccante sta cercando di chiamare ricorsivamente. L'esempio di codice precedente è un attacco di rientranza a funzione singola.
* Attacco di rientranza a funzioni incrociate (Cross-function reentrancy attack)
  + Questi attacchi sono più difficili da rilevare. Un attacco di tipo cross-function reentrancy è possibile quando una funzione vulnerabile condivide lo stato con un'altra funzione che ha un effetto desiderato dall'attaccante. Vediamo il seguente esempio.

Immagine che contiene testo

Descrizione generata automaticamente

In questo esempio, *withdraw* chiama la funzione di fallback dell'attaccante, come nel caso dell'attacco di rientranza a funzione singola.

La differenza è che la funzione di fallback effettua una chiamata a transfer invece di chiamare ricorsivamente *withdraw*. Poiché il saldo non è stato impostato a 0 prima di questa chiamata, la funzione *transfer* può trasferire un saldo che è già stato speso.

* Soluzioni possibili 🡪 Ci sono alcune best practices da seguire per proteggere gli smart contracts
  + *Send, Transfer* e *Call*
    - Poiché la maggior parte degli attacchi di rientranza coinvolge funzioni di *send*, *transfer* o *call*, è importante capire la differenza tra di esse.
    - Le funzioni *send* e *transfer* sono considerate più sicure perché sono limitate a 2.300 gas. Il limite di gas impedisce le costose chiamate di funzioni esterne al contratto di destinazione. L'unica insidia è quando un contratto imposta una quantità di gas personalizzata per un invio o un trasferimento utilizzando *msg.sender.call(ethAmount).gas(gasAmount*).
    - La funzione *call* è purtroppo molto più vulnerabile.
    - Quando si prevede che una chiamata di funzione esterna esegua operazioni complesse, in genere si vuole usare la funzione *call* perché inoltra tutto il gas rimanente. Questo apre la porta a un attaccante che può richiamare la funzione originale in un attacco di rientranza a funzione singola o una funzione diversa dal contratto originale in un attacco di rientranza a funzione incrociata.
    - Ove possibile, utilizzare *send* o *transfer* al posto di call per limitare il rischio di sicurezza.
  + Contrassegnare le funzioni non attendibili
    - Per proteggersi dagli attacchi di reentrancy, è importante identificare quando una funzione non è attendibile. Le best practices di Consensys (azienda leader nella formazione blockchain) consigliano di denominare le funzioni e le variabili in modo da indicare se non sono attendibili. Ad esempio:

Immagine che contiene testo

Descrizione generata automaticamente

* + - È importante ricordare che se una funzione chiama un'altra funzione non attendibile, è anch'essa non attendibile.
  + Schema controlli-effetti-interazioni (Checks-effects-interactions pattern)
    - Il metodo più affidabile per proteggersi dagli attacchi di rientranza è l'uso dello schema checks-effects-interactions. Questo schema definisce l'ordine in cui strutturare le funzioni.
    - Prima si eseguono i controlli, che di solito sono dichiarazioni assert e require, all'inizio della funzione. Se i controlli passano, la funzione deve poi risolvere tutti gli effetti allo stato del contratto.
    - Solo dopo che tutti i cambiamenti di stato sono stati risolti, la funzione deve interagire con altri contratti. Chiamando le funzioni esterne per ultime, anche se un attaccante effettua una chiamata ricorsiva alla funzione originale, non può abusare dello stato del contratto.
    - Riscriviamo la nostra funzione di prelievo vulnerabile utilizzando lo schema controlli-effetti-interazioni.

Immagine che contiene testo

Descrizione generata automaticamente

* + - Poiché azzeriamo il saldo - un effetto - prima di effettuare una chiamata esterna, una chiamata ricorsiva effettuata da un attaccante non sarà indotta a pensare che ci sia ancora un saldo residuo.
  + Mutex
    - In situazioni più complesse, come la protezione dagli attacchi di rientranza tra funzioni, può essere necessario utilizzare un mutex. Un mutex pone un blocco sullo stato del contratto. Solo il proprietario del blocco può modificare lo stato.

Immagine che contiene testo, lettera

Descrizione generata automaticamente

* + - Utilizzando questo blocco, un aggressore non può più sfruttare la funzione withdraw con una chiamata ricorsiva. Né un aggressore può sfruttare una chiamata al trasferimento per un attacco di rientranza tra funzioni. Tutte le modifiche allo stato avvengono quando il blocco è vero, impedendo a qualsiasi funzione che controlla il blocco di essere chiamata fuori ordine.
    - È necessario prestare attenzione all'implementazione di un mutex per assicurarsi che ci sia sempre un modo per rilasciare un blocco. Se un attaccante riesce a ottenere un blocco sul contratto e a impedirne il rilascio, il contratto può essere reso inerte.

* DoS (Denial of Service)
  + Supponiamo che a un certo punto della logica del codice si invochi una funzione di un contratto esterno e che, se l'invocazione ha successo, si prosegua con l'esecuzione del codice. Se per qualche motivo uno sviluppatore malintenzionato ha implementato la funzione del contratto esterno in modo che fallisca sempre, la parte finale della funzione non verrà mai eseguita, effettuando un attacco DoS in piena regola
* Soluzione: Presupporre sempre che le chiamate esterne possano fallire. Se possibile, implementare uno schema "pull" invece di uno "push".
  + In uno schema "push", i contratti invocano la funzione del proprio codice che invocherà un contratto di terze parti. In questo modo un contratto maligno potrebbe bloccare altri utenti.
  + In uno schema "pull", i contratti invocano la funzione del proprio codice, che in cambio invocherà solo la funzione del contratto chiamante. In questo modo, se uno sviluppatore malintenzionato tenta di fare un DoS alla vostra funzione, bloccherà solo sé stesso e non gli altri utenti.
* Replay signature attacks (Attacchi con firme di replay)
  + Le firme sono un modo per un conto di inviare le transazioni di un altro conto alla blockchain. Il conto originale firmerà un messaggio e il conto di consegna invierà il messaggio a uno smart contract, in modo che sia il conto di consegna a pagare le spese di transazione e non il conto originale.
  + Naturalmente lo smart contract deve avere funzioni in grado di convalidare le firme e di eseguire i compiti richiesti.
  + Tuttavia, se un messaggio firmato è valido e il vostro smart contract ne eseguirà il contenuto, chiunque avrà accesso ad esso (letteralmente chiunque monitori la blockchain) potrebbe inviarlo più volte, il che significa che la funzionalità dello smart contract potrebbe essere eseguita più volte per lo stesso messaggio, cosa che non era nelle intenzioni dell'account originale quando ha firmato il messaggio.
* Soluzione: Aggiungere un nonce per account ai messaggi firmati. I messaggi firmati dallo stesso account con un nonce già utilizzato non vengono accettati. Ogni volta che un account firma un nuovo messaggio, dovrà incrementare il nonce. Lo standard EIP-712 può aiutare in questo senso.
* Definire sempre la visibilità di default delle funzioni, specie per tenere private le funzioni che devono esserlo
* Definire sempre una specifica versione di pragma di Solidity
* Cercare sempre di usare i mapping quando si prevede un lungo elenco di valori
* Ereditarietà sbagliata
  + Solidity supporta eredità multiple che introducono l'ambiguità chiamata "problema del diamante". In pratica, se più contratti padre implementano la stessa funzione, occorre capire quale contratto sarà chiamato
  + Solidity utilizza la linearizzazione C3 per stabilire le priorità tra i contratti padre. Se non si presta attenzione a questo aspetto, si potrebbero avere comportamenti inaspettati. Esso garantisce che si consideri l’ordine di definizione delle classi e la relazione di ereditarietà tra di esse. In pratica, l'algoritmo crea una lista ordinata di tutte le classi coinvolte nell'ereditarietà, in modo che ogni classe appaia solo una volta nella lista e rispetti l'ordine di definizione delle classi.
* Soluzione: Come regola generale, si aggiungono i contratti padre partendo da quello più generico a quello più specifico.
* Saldo inatteso di ether
  + Si potrebbe pensare che l'unico modo per il proprio contratto di ricevere etere sia quello di implementare funzioni "payable" e/o una funzione di receive. Ma anche se il contratto non ha assolutamente funzioni " payable " e non ha funzioni di receive, potrebbe comunque riceverne nelle due situazioni seguenti:
    - Come risultato di una "autodistruzione" di un altro contratto. Ogni volta che un contratto si autodistrugge può decidere a quale conto inviare il suo saldo corrente.
    - Come risultato di un nuovo ether estratto. Ogni volta che un miner aggiunge un blocco alla blockchain riceverà una ricompensa in ether, il miner può decidere a quale conto assegnare l'ether.
    - Questi due tipi di trasferimento di ether non saranno comunque catturati dalla funzione receive
* Soluzione: Non pensare mai di poter memorizzare in una variabile di stato la quantità esatta di ether che il vostro contratto possiede semplicemente reagendo alle transazioni ricevute. Nel migliore dei casi, si sarà in grado di memorizzare la quantità minima che possiede.
* Accesso al di fuori dei limiti dell'array
  + Nelle prime versioni di Solidity, le lunghezze degli array dinamici di memorizzazione potevano essere modificate direttamente (senza aggiungere o rimuovere elementi). Il problema è che le variabili di stato condividono lo stesso spazio di memorizzazione, il che significa che se si lascia che gli utenti modifichino la lunghezza di un array, possono potenzialmente accedere a qualsiasi slot nello spazio di memorizzazione, e potrebbero sostituire qualsiasi variabile di stato nel contratto, anche quelle a cui non dovrebbero avere accesso.
* Soluzione: Utilizzare una versione di Solidity priva di questa vulnerabilità o semplicemente non consentire agli utenti di modificare le lunghezze degli array di storage.
* Delegare le chiamate a fonti non attendibili
  + Questa è probabilmente la più grande vulnerabilità di sicurezza che si possa avere. Le "chiamate delegate" invocano una funzione di un contratto esterno e la eseguono all'interno del contesto del contratto (a differenza delle normali chiamate che vengono eseguite nel contesto del chiamante). Il contratto esterno avrà pieno accesso alle variabili di stato e potrà fare ciò che vuole.
  + Soluzione: Usare con attenzione le chiamate ai delegati.
* Chiamate (regolari) a fonti non attendibili
  + Anche le chiamate a contratti non attendibili possono avere risultati inaspettati. Si tenga presente che richiamare due volte la funzione dello stesso contratto può restituire due risultati diversi, per esempio, si chiama una funzione di un contratto non attendibile "check\_condition\_X()" che inizialmente può restituire true, ma se la si richiama subito dopo (nulla nel contratto è cambiato nel frattempo e siamo ancora nella stessa transazione) potrebbe restituire false (lo stato del contratto non attendibile potrebbe essere cambiato a causa della prima invocazione).
* Soluzione: Se nel codice è necessario un valore fornito dall'esterno, invece di richiamare ogni volta il contratto esterno, salvare il valore in una variabile locale.
* Casualità insicura
  + Per definizione, i contratti intelligenti devono essere deterministici, devono restituire lo stesso risultato ogni volta che li eseguiamo, il che significa che, sempre per definizione, la casualità non è possibile.
* Soluzione: La soluzione più semplice è di non includere la casualità nel contratto smart, ma se si deve farlo, dipende da quanto deve essere sensibile il valore casuale. Potenzialmente si potrebbero usare variabili globali (timestamp del blocco, numero del blocco, ...) o usare un oracolo come Chainlink per ottenere una casualità sicura.
* Manipolazione del timestamp del blocco
  + I minatori scelgono il timestamp del blocco che estraggono, non possono impostare qualsiasi timestamp, ma hanno una certa flessibilità. Se state implementando uno smart contract che richiede valori di data e/o ora per funzionare correttamente, i minatori potrebbero avere la possibilità di violarlo.
* Soluzione: È possibile lavorare con i dati e l'ora a patto di non essere troppo restrittivi. Come regola generale, si dovrebbe essere in grado di tollerare una variazione di almeno 15 secondi.
* Contratti con codice zero
  + È possibile verificare se un conto corrisponde a uno smart contract o se è di proprietà esterna. Il modo per farlo è controllare la "dimensione del bytecode" relativa all'account (utilizzando l'assembly). Gli account hanno diverse proprietà in Ethereum (saldo, nonce, ecc.), e una di queste è il "bytecode", che è vuoto per un account di proprietà esterna e contiene alcuni dati per gli smart contract.
  + Tuttavia, durante la distribuzione di un nuovo contratto, la funzione "costruttore" del contratto verrà eseguita prima della creazione dello smart contract, il che significa che durante questo processo di esecuzione, l'indirizzo dello smart contract non avrà alcun "bytecode" collegato. Se uno smart contract invoca la vostra funzione mentre è stato distribuito, non verrà rilevato come smart contract ma come account di proprietà esterna.
* Soluzione: Se avete bisogno di limitare l'accesso al vostro smart contract, il modo migliore sarebbe quello di avere una whitelist, ma se davvero si ha bisogno di impedire agli smart contract di invocare il codice del proprio contratto, forse il modo migliore sarebbe quello di controllare se "msg.sender" corrisponde a "tx.origin", dato che l’account originale di una transazione deve sempre essere un conto di proprietà esterna.
* Puntatori di memoria non inizializzati
  + Questa è per lo più una buona pratica. Inizializzare sempre la variabile di stato (dal costruttore o dalla funzione di inizializzazione, se si utilizzano proxy trasparenti), altrimenti i valori vuoti predefiniti potrebbero portare a comportamenti inaspettati.
* Soluzione: Fortunatamente dalla versione 0.5.0 di Solidity i puntatori di stato devono essere inizializzati.
* Contratti intelligenti non aggiornabili
  + I contratti intelligenti sono per definizione immutabili (possono essere "autodistrutti" non modificati) e inarrestabili, il che significa che se per qualche motivo si distribuisce un contratto intelligente difettoso, non sarà possibile correggerlo e distribuire nuovamente una nuova versione...
* Soluzione: Utilizzate sempre modelli aggiornabili per i propri smart contract (usando il design pattern Proxy, con implementazioni quali proxy trasparenti, admin proxy, beacon proxy, ecc.). Si può anche considerare la possibilità di aggiungere lo schema "Pausable" ad alcune funzioni del contratto. Le funzioni "Pausable" possono essere messe in pausa (il che significa che nessuno può invocarle), il che darà più tempo per risolvere un bug e distribuire una nuova versione.
* Implementazioni logiche inizializzabili
  + Per avere contratti intelligenti aggiornabili, come detto il pattern "proxy" viene utilizzato molto spesso. L'idea è semplice, in poche parole: viene distribuito un contratto "logico" (con tutto il codice byte dell'EVM), quindi vengono distribuiti uno o più contratti "proxy", configurati per delegare tutte le loro chiamate al contratto logico. I proxy non contengono alcuna logica, tutto il codice è nel contratto logico, tuttavia i proxy mantengono la propria variabile di stato.
  + In molti di questi casi è necessario "inizializzare" i proxy. L'inizializzazione di un contratto viene normalmente effettuata tramite la funzione "costruttore", che viene eseguita una sola volta (durante la distribuzione), ma se viene implementato il "modello proxy", i costruttori non possono essere utilizzati, poiché inizializzerebbero la logica e non i proxy. Per questo motivo, per inizializzare un proxy, i contratti logici espongono un metodo *initialize* che può essere chiamato da chiunque e che imposta lo stato iniziale del contratto. I proxy chiamano questo metodo (utilizzando una chiamata delegata come per qualsiasi altro metodo logico) e inizializzano il proprio stato.
  + La vulnerabilità deriva dal fatto che il metodo initialize può essere chiamato da chiunque, il che significa che chiunque potrebbe potenzialmente inizializzare il contratto logico stesso. All'inizio questo non è un problema, poiché i proxy si affidano al contratto logico per il codice byte eseguibile, non per lo stato, poiché mantengono il proprio, e l'inizializzazione dello stato logico non avrebbe un impatto su nessuno dei proxy.
  + Tuttavia, in alcuni casi, potrebbe accadere che un aggressore possa impostare lo stato del contratto logico in modo da avere la possibilità di distruggerlo, ad esempio se il contratto logico effettua una chiamata di delega a un indirizzo incluso nel suo stato che può essere impostato solo da un amministratore.
  + L'account dell'amministratore sarà probabilmente impostato attraverso il metodo initialize; un aggressore potrebbe quindi rivendicare l'amministrazione del contratto logico e impostare l'indirizzo della chiamata delegata a un contratto che esegua semplicemente il comando "autodistruzione". In questo caso, il contratto logico verrebbe rimosso e i proxy resterebbero "puntati" a un contratto vuoto.
* Soluzione: La soluzione è in realtà piuttosto semplice. Quando si distribuisce il contratto logico, si dovrebbe includere un metodo costruttore, il cui scopo sarebbe semplicemente quello di impostare il flag di inizializzazione su false. L'idea è che il metodo initialize non sia eseguibile nel contesto del contratto logico stesso, ma solo attraverso chiamate di delegati.
* Attacco Flashloan
  + I Flashloans consentono agli utenti di prendere in prestito enormi quantità di criptovalute con una sola e rapida transazione. In altre parole, con un flashloan un utente può prendere in prestito una grande quantità di criptovaluta (come Ethereum o Bitcoin) per un breve periodo di tempo (generalmente poche ore), e poi restituire il prestito insieme agli interessi. Ciò può essere fatto senza la necessità di fornire alcuna garanzia, poiché il prestito viene concesso solo per un breve periodo di tempo e viene restituito in una sola transazione.
  + Grazie alla loro adattabilità e accessibilità, non richiedono garanzie e possono essere utilizzati per una moltitudine di scopi. Tuttavia, poiché non richiedono alcuna garanzia, i flashloan possono essere utilizzati per manipolare il mercato o sfruttare le debolezze degli smart contract.
  + Esempio di exploit Beanstalk DeFi (17 aprile 2022). Beanstalk è un protocollo decentralizzato di stablecoin che premia gli utenti che contribuiscono con fondi a un pool di finanziamento centrale chiamato "silo". Il protocollo mantiene il token "bean" a circa 1 dollaro. Inoltre, Beanstalk presenta una struttura di governance che consente ai titolari di token di votare per modificare il codice, con un potere di voto proporzionale al numero di token posseduti. Questa struttura di governance ha portato a una vulnerabilità del sistema che ha causato la caduta del progetto.
  + L’attaccante ha creato due proposte. Una era la richiesta di inviare tutti i fondi al proprio indirizzo. L'altra consisteva nel donare 250000 dollari in gettoni BEAN all'Ucraina. E qui arriva la parte difficile: la funzione emergencyCommit consente agli utenti con la super maggioranza dei fondi di approvare una proposta.
  + Il protocollo ha dimenticato di prendere le precauzioni per i flashloan consentendo l'hack appena un giorno dopo la proposta malevola. L'exploiter ha ottenuto un massiccio flashloan: 350 milioni di DAI, 500 milioni di USDC, 150 milioni di USDT, 32 milioni di Bean e 11,6 milioni di LUSD. Li ha convertiti in token BEAN3Crv-f e BEANLUSD-f della governance di Beanstalk DeFi. Raggiunta la maggioranza del 78% dei fondi, hanno chiamato emergencyCommit per eseguire entrambe le proposte che avevano creato.
* Soluzioni
  + Richiedere garanzie per i prestiti per rendere più costoso per gli hacker prendere in prestito le risorse.
  + Implementare limiti sulle dimensioni dei prestiti flash che possono essere sottoscritti, il che può aiutare a mitigare gli attacchi su larga scala.
  + Aggiungere blocchi temporali ai contratti intelligenti per impedire la possibilità di rimborsare i prestiti flash troppo velocemente, dando agli sviluppatori il tempo di rilevare e prevenire gli attacchi.
  + Inoltre, i progetti con sistemi di votazione della governance devono implementare un meccanismo anti-flashloan per impedire agli sfruttatori di utilizzare i flashloan per ottenere la maggioranza del potere di voto.
* Limite di dimensione dello stack
  + Fino a un hard fork, era possibile creare una lunga catena di chiamate (una in meno del limite) e poi chiamare un contratto vittima. Se la vittima chiamava qualche altra funzione, questa falliva con un'eccezione dovuta al limite di dimensione dello stack. Il contratto vittima potrebbe non aspettarsi un'eccezione.
* Front running
  + È interessante notare che i contratti intelligenti e le transazioni diventano completamente pubblici una volta inviati alla rete come transazione in sospeso. Queste transazioni sono visibili all'intera rete nelle mempool dei nodi Ethereum, consentendo ai minatori di blocchi di selezionare le transazioni con le tariffe di gas più elevate. Questa visibilità ha un effetto collaterale significativo. Permette ad attori malintenzionati di vedere il risultato previsto di uno smart contract prima che venga confermato sulla blockchain.
  + Il front running è una pratica dannosa che si verifica quando un utente sfrutta la conoscenza anticipata di una transazione in arrivo per eseguire una transazione correlata con lo stesso contratto, in modo da ottenere un vantaggio sui concorrenti. In altre parole, l'utente malintenzionato utilizza informazioni riservate sulle transazioni in arrivo per eseguire una transazione in anticipo e trarre un profitto.
* Soluzioni
  + Esistono diverse soluzioni per affrontare il problema, quali:
    - Zero-knowledge Proofs: Sono un meccanismo crittografico che consente a un utente di dimostrare di avere accesso a una determinata informazione senza rivelare la stessa informazione agli altri utenti. In questo modo, gli utenti possono dimostrare di avere accesso a una transazione senza rivelare la stessa transazione agli altri utenti.
    - Auction Mechanisms: l'utilizzo di meccanismi di asta può aiutare a mitigare il front running, in quanto gli utenti sono tenuti a fare offerte senza conoscere le offerte degli altri utenti. In questo modo, gli utenti non possono conoscere le offerte degli altri utenti e non possono quindi eseguire transazioni in anticipo.
    - Randomness: l'introduzione di elementi di casualità nelle transazioni può rendere più difficile prevedere quando avverranno le transazioni e ridurre il rischio di front running.
    - Off-Chain Matching: l'utilizzo di sistemi di matching off-chain può ridurre il rischio di front running, in quanto le transazioni sono eseguite al di fuori della blockchain, in modo che gli utenti non possano vedere le transazioni degli altri utenti.

# Self Sovereign Identity

La self-sovereign identity (SSI) è un approccio all'identità digitale che dà agli individui il controllo sulle informazioni che usano per dimostrare chi sono a siti web, servizi e applicazioni in tutto il web. Senza l'SSI, gli individui con account (identità) persistenti su Internet devono affidarsi a una serie di grandi fornitori di identità, come Facebook, Google, etc. che hanno il controllo delle informazioni associate alla loro identità. Se un utente sceglie di non utilizzare un grande fornitore di identità, deve creare nuovi account con ogni fornitore di servizi, frammentando la sua esperienza sul Web. In un sistema di identità auto-sovrana (SSI), l'utente accede ai servizi in modo snello e sicuro, mantenendo il controllo sulle informazioni associate alla propria identità.

La tecnologia SSI consente alle persone di autogestire la propria identità digitale senza dipendere da fornitori terzi per l'archiviazione e la gestione dei dati. Attualmente, il termine Self-Sovereign Identity è usato in modo intercambiabile con il termine identità decentralizzata.

Esistono molti modi per implementare l'SSI utilizzando le chiavi crittografiche e ne analizzeremo due.

* Utilizzo di un identificatore digitale unico (DID)

In questa implementazione, insieme alla coppia di chiavi private e pubbliche viene generato anche un identificatore digitale univoco (in genere un numero grande). È necessario registrare la chiave pubblica e l'identificatore digitale unico sulla blockchain, mentre la chiave privata può essere conservata in un portafoglio digitale.

Al momento dell'autenticazione, il sistema cerca l'identificatore unico e la chiave pubblica associata, mentre l'utente dimostra la proprietà di questo identificatore con la sua chiave privata.

* Utilizzo di firme digitali

Un'altra implementazione è costituita da identificatori decentralizzati e credenziali verificabili.

Le parti coinvolte in questo processo sono tre:

* Emittente - L'entità che emette una credenziale, ad esempio un documento d'identità governativo.
* Titolare - Il proprietario della credenziale, cioè l'entità su cui l'emittente genera la credenziale.
* Verificatore - L'entità che controlla la validità e l'autenticità della credenziale presentata dal titolare.

L'emittente firma una credenziale verificabile con la propria chiave privata, la cripta con la chiave pubblica del titolare e la invia a quest'ultimo. Successivamente, il titolare memorizza questa VC in un portafoglio di identità e può decifrarla utilizzando la propria chiave privata per accedere alla VC.

Al momento della verifica, il titolare crea una presentazione verificabile che può includere una o più credenziali, la firma digitale con la propria chiave privata e la cripta con la chiave pubblica del verificatore. Il verificatore decifra la VC e ne verifica l'autenticità utilizzando le chiavi pubbliche del titolare e dell'emittente.

Le interazioni tra titolare, emittente e verificatore sono talvolta chiamate "triangolo della fiducia". Ogni volta che un verificatore richiede informazioni, il titolare sceglie se consentire l'accesso ai propri dati.

## Principi base

Ci sono una serie di principi base nella SSI:

* Esistenza - Gli utenti devono avere un'esistenza indipendente, senza aver bisogno di un provider di terze parti.
* Controllo - Gli utenti devono controllare la propria identità. In questo modello, l'utente deve poter controllare la propria identità. Deve essere sempre in grado di visualizzarla, aggiornarla o addirittura nasconderla.
  + In genere, per far valere questo principio, esercitare il controllo sulla propria identità richiede l'appoggio dello Stato o di altre terze parti. La Blockchain risolve il problema del controllo utilizzando algoritmi sicuri che aiutano gli utenti a garantire la validità continua dell'identità e delle richieste associate. Questo metodo elimina la necessità di un controllo compromesso da parte di entità come lo Stato o terze parti.
* Accesso - Gli utenti devono avere accesso ai propri dati. L'utente deve essere sempre in grado di accedere ai propri dati, non ci possono essere dati nascosti o inaccessibili della propria identità. D'altra parte, l'utente deve poter accedere solo alla propria identità e non a quella degli altri.
  + Ciò non significa necessariamente che l'utente abbia l'autorità di modificare tutti gli aspetti e le rivendicazioni associate alla sua identità; significa, tuttavia, che un utente dovrebbe essere in grado di accedere alle registrazioni che indicano qualsiasi modifica associata alla sua identità. Per proteggere la sovranità degli altri utenti, a un individuo dovrebbe essere concesso l'accesso solo alla propria identità e non a quella degli altri.
* Trasparenza - I sistemi e gli algoritmi devono essere trasparenti.
  + Il modo in cui un sistema di identità e gli algoritmi sono gestiti e aggiornati deve essere pubblicamente disponibile e ragionevolmente comprensibile. La progettazione della soluzione deve basarsi su standard di protocollo e software aperti.
* Persistenza - Le identità devono avere una vita lunga. Questo principio sostiene che le identità dovrebbero essere durature, a discrezione dell'utente. In presenza di continui cambiamenti nell'archiviazione dei dati e nella rotazione delle chiavi private (se un utente possiede più portafogli o identificatori nell'ambito di una blockchain), la persistenza consente agli utenti di mantenere la propria identità, pur avendo più chiavi private.
  + Per qualsiasi piattaforma SSI, i cambiamenti nella memorizzazione dei dati e nella rotazione delle chiavi private dovrebbero resistere agli aggiornamenti del sistema e, idealmente, essere interoperabili con altri sistemi e algoritmi.
* Portabilità - Le informazioni e i servizi sull'identità devono essere trasportabili tra piattaforme diverse, senza essere costretti da una specifica. Le informazioni e i servizi relativi all'identità devono essere facilmente trasportabili per garantire che l'identità di un utente possa essere trasferita e archiviata in più luoghi, a seconda delle necessità. Le informazioni devono essere disponibili in tutto il mondo, senza che l'utente perda il controllo della propria identità.
* Interoperabilità - Le identità devono essere il più possibile utilizzabili. Organizzazioni, database e registri devono essere in grado di comunicare tra loro in modo rapido ed efficiente a livello globale attraverso un sistema di identità digitale.
* Consenso - Gli utenti devono acconsentire all'uso della loro identità. I sistemi SSI richiedono che la condivisione dei dati personali avvenga solo con il consenso dell'utente. Quando si costruisce un'identità auto-sovrana decentralizzata, il consenso deve essere sempre tenuto presente e incorporato nel sistema. Questo garantisce che i dati dell'identità rimangano privati o meno (a discrezione dell'utente).
  + Attraverso un consenso deliberatamente progettato, ogni transazione di dati di identità sarà eseguita solo con il consenso dell'utente. Questa innovazione di autenticazione reciproca significa che entrambe le parti firmeranno le rispettive richieste, consentendo a ciascuna di esse di creare una registrazione dell'interazione dei dati. In questo modo si crea una piena autonomia dell'utente, che avrà il pieno controllo di dove i suoi dati di identità vengono condivisi o scambiati.
* Minimizzazione - La divulgazione delle richieste deve essere ridotta al minimo. Questo principio sottolinea l'importanza di proteggere i dati personali degli utenti quando si divulgano informazioni relative all'identità.
  + Ad esempio, se viene richiesta l'età minima di un utente (per accedere a una pagina), non si deve chiedere all'utente di fornire il giorno, il mese e l'anno di nascita precisi. Al contrario, la divulgazione da parte dell'utente dovrebbe essere ridotta al minimo fornendo il requisito minimo (anni di età).
  + Anche il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea si è espresso a favore della minimizzazione dei dati. L'ente normativo sottolinea come l'elaborazione dei dati debba utilizzare solo la quantità di dati necessaria per portare a termine un determinato compito.
* Protezione - I diritti degli utenti devono essere protetti. Il diritto alla privacy delle persone deve essere protetto e devono esistere garanzie contro la manomissione e il monitoraggio delle informazioni. Il traffico di dati deve essere criptato end-to-end.

Il modello dei dati è passato da un modello puramente centralizzato da singole organizzazioni ad n modello di completamente federato e mantenuto completamente da singole organizzazioni, fino all’idea di spingere l’utente ad avere il pieno controllo di tutti i propri dati

## Componenti dell’architettura

1. Blockchain

La blockchain, come sappiamo a questo punto, di base è una rete decentralizzata in cui ciascun nodo tiene traccia di tutte le transazioni senza che queste vengano alterate (immutabilità).

Ecco come ogni parte utilizza la blockchain in un sistema di identità auto-sovrana:

* Titolare (Holder): Il titolare della credenziale verificabile (ad esempio, la patente di guida) ha il suo DID pubblico sulla blockchain.
* Emittente (Issuer): quando un emittente, come un dipartimento governativo, fornisce una Credenziale verificabile a un titolare, come una patente di guida, la firma con il proprio DID e la chiave privata associata. Il DID del dipartimento e la chiave pubblica associata saranno presenti sulla blockchain.
* Verificatore (Verifier): Un verificatore, come una società di guida su richiesta, può controllare la blockchain per assicurarsi che il dipartimento governativo di cui si fida abbia effettivamente rilasciato la patente perché la credenziale è stata firmata dal DID dell'emittente che si trova sulla blockchain.

Una blockchain consente al titolare, all'emittente e al verificatore di avere la stessa fonte di verità su quali credenziali sono valide e su chi ha autenticato la validità dei dati contenuti nelle credenziali. Tramite l’utilizzo della crittografia a chiave pubblica si dimostra l’identità attraverso la firma digitale sui messaggi e relativo scambio di chiavi.

1. Decentralized Identifiers (DIDs)

Un DID è un identificativo unico a livello globale composto da una stringa di lettere e numeri, indipendente da qualsiasi organizzazione. I DID sono conosciuti pubblicamente dalle parti interessate. Le persone possono creare tutte le DID che vogliono per scopi e interazioni diverse.

Ciascun DID:

* Viene creato dall'utente
* Viene fornito con una o più coppie di chiavi private e pubbliche
* Non contiene dati personali o informazioni sul portafoglio
* Consente connessioni private e sicure tra due parti e può essere verificato ovunque e in qualsiasi momento

In merito alle chiavi:

* Chiave privata: Costituita da una lunga serie di lettere e numeri che consente di dimostrare la proprietà, dare il consenso alla condivisione di dati selezionati e firmare credenziali verificabili. Per analogia, una chiave privata è come una chiave principale che può accedere a tutte le vostre informazioni e il proprietario non dovrebbe mai condividere la sua chiave privata con nessuno.
* Chiave pubblica: Costituita da una lunga stringa di lettere e numeri che può essere tranquillamente condivisa con chiunque decida di fornire informazioni specifiche.

1. Verifiable Credentials

Le credenziali verificabili sono una versione digitale e crittograficamente protetta delle credenziali cartacee e digitali che le persone possono presentare alle parti che ne hanno bisogno per la verifica. Un datore di lavoro, ad esempio, può semplicemente utilizzare un'app per scansionare il codice QR di un candidato al lavoro e confermare che ha conseguito una laurea, senza dover passare giorni o settimane a contattare un'università per verificare l'autenticità del titolo di studio.

Il Verifiable Credentials Data Model 1.0 è una "specifica [che] fornisce un modo standard per esprimere le credenziali sul Web in un modo crittograficamente sicuro, rispettoso della privacy e verificabile dalle macchine". Il W3C ha creato standard per gli identificatori decentralizzati, gli URL e altri.

Vi sono alcuni sensibili vantaggi nel loro utilizzo:

* Organizzazioni emittenti: Risparmio di denaro e di tempo nell'emissione di credenziali verificabili in modo efficiente, con la possibilità di emettere in blocco, prevenire le frodi e ridurre il lavoro manuale.
* Organizzazioni che verificano: Risparmio di tempo, risorse e denaro grazie alla verifica istantanea delle credenziali senza dover contattare le organizzazioni emittenti.
* Individui: Forniscono solo le informazioni rilevanti a un verificatore senza rivelare informazioni inutili e confermano le richieste senza rivelare i dati reali.
* Sviluppatori: Migliorano l'esperienza dell'utente autenticandosi in modo sicuro senza bisogno di password.

Ci sono due modi principali in cui le società blockchain di identità sovrana possono consentire alle persone di preservare la privacy:

* Selective Disclosure (Divulgazione selettiva)

È possibile decidere quali dati di una credenziale mostrare a un verificatore senza rivelare informazioni non necessarie rispetto a quelle richieste. Ad esempio, se è necessario avere almeno 18 anni per ricevere un servizio, si può mostrare la data di nascita dalla patente che è stata rilasciata come credenziale verificabile senza mostrare il proprio nome o indirizzo.

* Zero-Knowledge Proofs (Prove a conoscenza zero - ZKP)

Con la tecnologia ZKP (Zero Knowledge Proof), i fornitori di identità sovrana si spingono ancora più in là per aiutare le persone a mantenere la privacy, dimostrando che avete 18 anni o più senza nemmeno rivelare la vostra data di nascita. Ciò è possibile grazie all'uso della crittografia, in cui il titolare può dimostrare al verificatore di soddisfare un determinato requisito (come l'età minima, il reddito o l'area di residenza) senza dover mostrare i dati che supportano tale prova.

Ecco un esempio abbastanza semplice e pratico di come vengono utilizzate le chiavi pubbliche e private nel sistema SSI.

* Titolare: Tommy
* Emittente: Dipartimento governativo
* Verificatore: Società di formazione inglese online

Un'azienda di formazione inglese online in Giappone vuole assumere insegnanti a contratto solo dagli Stati Uniti e dal Canada. Utilizza credenziali verificabili come parte del processo di screening per garantire che gli insegnanti siano residenti in Nord America.

* Tommy ha una DID nel suo Wallet e vuole aggiungervi i dati del suo passaporto.
* Tommy si reca all'ufficio governativo e il personale gli chiede di scansionare un codice QR, che consente una connessione sicura e lo scambio di DID.
* Il personale utilizza la chiave privata per firmare e rilasciare il passaporto digitale come credenziale verificabile.
* Tommy accetta la credenziale e la memorizza nel suo portafoglio.
* La società di formazione online richiede i dati per confermare che vive in Canada o negli Stati Uniti.
* Tommy autorizza l'azienda di formazione online a vedere i suoi dati rilevanti.
* L'azienda verifica la credenziale che conferma la sua residenza in Canada.

1. Wallet digitale

Un portafoglio sicuro per la SSI è essenziale perché consente alle persone di portare le proprie credenziali ovunque sul proprio telefono o dispositivo digitale. La portabilità è uno dei principi della SSI.

Vi sono alcuni aspetti chiave per un wallet SSI:

* Consente alle persone di memorizzare e gestire in modo sicuro le DID e le credenziali verificabili senza affidarsi a terzi.
* Il titolare deve dare l'autorizzazione a condividere i dati a un verificatore che deve confermare l'idoneità ad accedere a servizi o prodotti.
* È più difficile per le aziende rintracciare o correlare le informazioni all'utente.
* Le persone possono accedere a siti web e app senza rivelare informazioni personali o più dettagli del necessario

Le persone possono accedere con una DID piuttosto che creare un nuovo account con nome utente e password per accedere a un altro sito web o app.

Se Sarah vuole acquistare alcolici e deve dimostrare di avere almeno 18 anni, può farlo senza rivelare la sua data di nascita o altri dettagli sulla sua identità utilizzando un portafoglio di identità sovrana che ha implementato la tecnologia di prova a conoscenza zero.

* Il cassiere richiede i dati del suo portafoglio che confermano che ha almeno 18 anni (con la patente di guida) e a Sarah viene chiesto di dare il permesso di condividere i dati.
* Quando Sarah approva la richiesta, si crea una connessione sicura tra il negozio e il portafoglio di Sarah durante lo scambio di DID.
* La patente di Sarah conferma che ha almeno 18 anni. Grazie alla tecnologia zero-knowledge proof, i dettagli della patente, come la data di nascita e il nome completo, non vengono affatto rivelati e il negozio si fida della legittimità dei dati forniti dall'emittente, l'organizzazione che ha rilasciato la patente. Un verificatore può utilizzare il DID dell'emittente e la chiave pubblica associata sulla blockchain per controllare che i dati nel portafoglio dell'utente siano autentici.

1. Standard di interoperabilità

Gli standard SSI che aiutano le persone a creare e gestire le proprie identità digitali sono un continuo lavoro in corso. Gli standard includono modelli di dati, codice open-source, API e altro ancora. Questi sono gli standard principali che sono stati sviluppati:

* W3C: Verifiable Claims Data Model and Representations v1.0

Il W3C Credentials Community Group studia la creazione, l'archiviazione, la presentazione, la verifica e il controllo delle credenziali da parte degli utenti. Il gruppo ha pubblicato una prima versione di Verifiable Claims Data Model and Representations 1.0 nel maggio 2017. La specifica discute i criteri delle affermazioni verificabili. Secondo questo standard, un'architettura auto-sovrana per le rivendicazioni verificabili è quella in cui il titolare di una rivendicazione verificabile ha il controllo completo del proprio identificatore e di come viene utilizzato.

* W3C DID: Decentralized Identifiers (DID) v1.0

Il gruppo di lavoro W3C DID ha stabilito gli standard per i DID in Decentralized Identifiers (DIDs) v1.0, in cui vengono specificati una serie di criteri, tra cui un modello di dati comune, le operazioni DID e una spiegazione del processo di risoluzione dei DID alle risorse che rappresentano.

Un DID identifica qualsiasi soggetto (ad esempio, una persona, un'organizzazione, una cosa, un modello di dati, un'entità astratta, ecc. Questi nuovi identificatori sono progettati per consentire al controllore di un DID di dimostrare il controllo su di esso e di essere implementati indipendentemente da qualsiasi registro centralizzato, fornitore di identità o autorità di certificazione. I DID sono URL che associano un soggetto DID a un documento DID che consente interazioni affidabili associate a quel soggetto.

Ogni documento DID può esprimere materiale crittografico, metodi di verifica o endpoint di servizio, che forniscono un insieme di meccanismi che consentono a un controllore DID di dimostrare il controllo della DID. Gli endpoint di servizio consentono interazioni affidabili associate al soggetto DID. Un documento DID può contenere la semantica del soggetto che identifica. Un documento DID può contenere il soggetto DID stesso (ad esempio, un modello di dati).

* Hyperledger Indy: software per ledger distribuiti

Hyperledger Indy fornisce strumenti, librerie e componenti riutilizzabili per fornire identità digitali radicate su blockchain o altri ledger distribuiti in modo che siano interoperabili tra domini amministrativi, applicazioni e qualsiasi altro silo. Indy è interoperabile con altre blockchain o può essere utilizzato in modo autonomo, favorendo la decentralizzazione dell'identità. Il repository di Indy è disponibile qui.

* Hyperledger Aries: protocolli per la comunicazione di VC e DID

Hyperledger Aries fornisce un kit di strumenti condivisi, riutilizzabili e interoperabili progettati per iniziative e soluzioni incentrate sulla creazione, la trasmissione e la conservazione di credenziali digitali verificabili (VC). È un'infrastruttura per interazioni peer-to-peer radicate nella blockchain. Il progetto si avvale del supporto crittografico fornito da Hyperledger Ursa, per fornire una gestione sicura dei segreti e funzionalità di gestione decentralizzata delle chiavi.

Hyperledger Aries consente interazioni peer-to-peer online basate su identità decentralizzate e credenziali verificabili. Aries include una definizione del protocollo, strumenti e implementazioni di riferimento. Il protocollo Aries supporta identità radicate in una varietà di libri mastri distribuiti o blockchain. Questo approccio all'identità è spesso chiamato Self Sovereign Identity (SSI).

I componenti chiave di una soluzione Aries sono:

* agenti,
* comunicazioni DID,
* protocolli,
* e gestione delle chiavi.

Inoltre, Hyperledger Aries sviluppa una serie di Request for Comment (RFC) che descrivono argomenti importanti da standardizzare nell'ecosistema Aries. Esistono due tipi di RFC di Aries:

* RFC che descrivono singole funzionalità (nella cartella delle funzionalità)
* RFC che spiegano i concetti alla base di molte funzionalità (nella cartella concepts).

Le RFC sono destinate agli sviluppatori che costruiscono su Aries. Non forniscono indicazioni su come i componenti di Aries implementano internamente le funzionalità; i singoli repo di Aries hanno documenti di progettazione per questo. Ogni RFC di Aries include una sezione "implementazioni" e tutte le RFC con uno stato superiore a Proposed dovrebbero avere almeno un'implementazione elencata.

* Hyperledger Ursa: libreria crittografica

Hyperledger Ursa è una libreria crittografica condivisa, che consente alle implementazioni di evitare la duplicazione di altro lavoro crittografico e, auspicabilmente, di aumentare la sicurezza nel processo. La libreria è un repository opt-in (per progetti Hyperledger e non) per inserire e utilizzare la crittografia. Hyperledger Ursa è costituito da sottoprogetti, che sono implementazioni coese di codice crittografico o interfacce per il codice crittografico.

* Decentralized Identity Foundation (DIF)

La Decentralized Identity Foundation è un'organizzazione di stampo ingegneristico che rappresenta una raccolta internazionale di organizzazioni e collaboratori che lavorano insieme per creare un ecosistema aperto di identità decentralizzata accessibile a tutti.

DIF si basa sul lavoro del W3C e di Hyperledger di cui sopra. Alcuni lavori provengono da Hyperledger Aries e sono stati trasferiti a DIF per una gestione più efficace dei diritti di proprietà intellettuale. Il DIF comprende, tra gli altri, i seguenti gruppi di lavoro:

* Identificatori e scoperta: Un elemento chiave dell'equazione dell'identità decentralizzata è il modo in cui le persone, le organizzazioni e i dispositivi possono essere identificati e localizzati senza sistemi centralizzati di identificatori (ad esempio, gli indirizzi e-mail). I membri del DIF stanno lavorando attivamente su protocolli e implementazioni che consentono la creazione, la risoluzione e la scoperta di identificatori e nomi decentralizzati in sistemi decentralizzati, come blockchain e libri mastri distribuiti.
* Archiviazione e calcolo: L'archiviazione e il calcolo sicuri, crittografati e rispettosi della privacy dei dati sono una componente critica dei sistemi di identità decentralizzati. Come gli identificatori e i nomi devono essere auto-sovrani rispetto all'entità proprietaria, i dati dell'identità di un utente devono rimanere privati, accessibili solo alle entità autorizzate. I membri del DIF stanno sviluppando attivamente le specifiche e le implementazioni di riferimento per le soluzioni run-anywhere e indipendenti dal provider che forniscono queste caratteristiche.
* Autenticazione: Progettazione e implementazione di specifiche, standard e librerie di autenticazione basate sui DID, utilizzate per autenticare i DID in un'ampia gamma di scambi e casi d'uso.
* Rivendicazioni e credenziali: La capacità di verificare le affermazioni e le dichiarazioni delle identità è fondamentale per stabilire la fiducia tra le entità in un sistema decentralizzato che non ha una gerarchia centralizzata. La DIF Foundation ha recentemente iniziato a definire le specifiche, i protocolli e gli strumenti che può fornire all'ecosistema per aiutare i partecipanti all'ecosistema e i loro clienti a integrare facilmente le asserzioni firmate DID nelle loro applicazioni e servizi.
* Comunicazione DID: Produrre una o più specifiche di alta qualità che incorporino un metodo ("DIDComm") per una comunicazione sicura, privata e (se del caso) autenticata basata su messaggi, in cui la fiducia è radicata nei DID e dipende dai messaggi stessi, non dalle proprietà esterne dei trasporti utilizzati.
* Archiviazione sicura dei dati: Creare una o più specifiche per stabilire un livello fondamentale per l'archiviazione sicura dei dati (compresi i dati personali), in particolare i modelli di dati per l'archiviazione e il trasporto, la sintassi, la protezione dei dati a riposo, le API CRUD, il controllo degli accessi, la sincronizzazione e almeno un'interfaccia minima valida basata su HTTP compatibile con i DID/VC del W3C.
* Sovrin: blockchain SSI

La Fondazione Sovrin è un'organizzazione privata internazionale senza scopo di lucro fondata per governare la prima rete di identità auto-sovrana (SSI) al mondo. La rete blockchain Sovrin è basata su Hyperledger Indy. Sovrin è governata dal Sovrin Governance Framework, che è un insieme di documenti ufficiali che includono accordi legali tra i partecipanti a Sovrin. I servizi di Sovrin sono registrazioni sulla blockchain Sovrin: DID e DID Documents, schemi VC (generici), definizioni VC (specifiche per l'emittente) e revoche VC. Dal 2017 al 2020, Sovrin è stata finanziata tramite donazioni (Sovrin Alliance) e la vendita dei futuri token SOV. Nel 2020, Sovrin ha avviato un processo di transizione, rivedendo il proprio finanziamento e la propria struttura.

* Trust-over-IP: governance full-stack

La fondazione Trust-over-IP è stata fondata a metà del 2020. Sta definendo un'architettura completa per la fiducia digitale su scala Internet che combina la fiducia crittografica a livello di macchina e la fiducia umana a livello aziendale, legale e sociale. Ha i seguenti gruppi di lavoro, oltre ad altri ancora in fase di avvio.

* Governance Stack: Lo scopo del gruppo di lavoro Governance Stack è quello di definire modelli e standard di interoperabilità per quadri di governance che consentano la fiducia commerciale, legale e sociale tra entità che implementano lo stack dell'architettura Trust over IP come definito nella RFC 0289 di Hyperledger Aries (o il suo successore come identificato nel documento RFC stesso).
* Technical Stack: Lo scopo del gruppo di lavoro Technical Stack è quello di definire (direttamente o per riferimento) gli standard tecnici, le suite di test e gli standard di certificazione dell'interoperabilità per lo stack architetturale Trust over IP come definito nella RFC 0289 di Hyperledger Aries (o il suo successore come identificato nel documento RFC stesso).
* Utility Foundry: Lo scopo del gruppo di lavoro Utility Foundry è quello di facilitare una comunità di pratica tra le autorità di governance, gli implementatori, gli operatori e i fornitori di servizi per le utility Trust over IP Layer One. Il gruppo di lavoro fornirà una guida al processo per la creazione e il monitoraggio di nuovi progetti di utilità ToIP Layer One, sia ospitati presso la Linux Foundation che esterni ad essa. Altre attività del WG comprendono la creazione di modelli di RFP per i fornitori di servizi, il mantenimento di un elenco di fornitori di servizi Foundry affiliati, l'identificazione di aree di collaborazione e allineamento tra utilità associate e/o disparate e, ove possibile, la funzione di centro di competenza per la formazione e la promozione del ruolo delle utilità ToIP Layer One.
* Ecosistema Foundry: L'obiettivo del gruppo di lavoro Ecosystem Foundry è quello di facilitare una comunità di pratica tra le autorità di governance, gli implementatori, gli operatori e i fornitori di servizi degli ecosistemi Trust over IP Layer Four. Il gruppo di lavoro fornirà una guida al processo per la creazione e il monitoraggio di nuovi progetti di ecosistemi ToIP Layer Four, sia ospitati presso la Linux Foundation che esterni ad essa. Altre attività del gruppo di lavoro comprenderanno la creazione di modelli di RFP per i fornitori di servizi, il mantenimento di un elenco di fornitori di servizi Foundry affiliati, l'identificazione di aree di collaborazione e allineamento tra ecosistemi associati e/o disparati e, ove possibile, la funzione di centro di competenza per la formazione e la promozione del ruolo degli ecosistemi ToIP Layer Four.

## Settori applicativi

* Smart cities

L'SSI svolge un ruolo importante nell'accelerazione dello sviluppo delle smart city. L'ID nazionale, il passaporto, la patente di guida, la prova di residenza, i documenti di identità degli studenti e altri VC possono favorire il viaggio di un cittadino nella sua città, semplificando la condivisione di corse sicure, il noleggio di veicoli, l'accesso ai trasporti pubblici, le strutture sportive e il check-in di eventi, per citarne alcuni. SSI dà potere al cittadino digitale e consente alle città intelligenti di avere una crescita e un impatto sostenibili.

* Viaggi e ospitalità

Essendo stato uno dei settori più colpiti dalla pandemia, l'industria dei viaggi e dell'ospitalità può sfruttare l'SSI per favorire la ripresa del settore.

Passaporti, visti, certificati di vaccinazione e carte fedeltà sono tra i VC che possono semplificare le attività di questo settore, tra cui, ma non solo, la sicurezza aeroportuale automatica, il check-in rapido delle compagnie aeree e il check-in istantaneo degli hotel. I casi d'uso per questo settore sono semplici e diretti, ma di grande impatto.

* Beni immobili

Il processo di affitto, acquisto e vendita di un immobile può essere noioso e richiede molte pratiche burocratiche da parte di tutte le parti coinvolte. Affittuari, acquirenti e venditori devono spesso fornire documenti come documenti d'identità nazionali, prove di residenza, dichiarazioni di reddito e atti immobiliari.

L'emissione di tali documenti come credenziali verificabili può ridurre questi lunghi processi a un istante e diminuire le possibilità di frode d'identità. Grazie all'ottimizzazione del processo, possono nascere nuove opportunità sul mercato, come gli scenari di compravendita P2P e l'accesso sicuro agli edifici.

* Istruzione

Le università possono essere sia emittenti che verificatori per le loro comunità. Il settore dell'istruzione superiore sta già implementando l'uso di diplomi accademici, ID studente, trascrizioni, certificati e altre micro-credenziali VC per trasformare le esperienze di studenti e personale e generare nuove opportunità per l'intero ecosistema.

L'onboarding istantaneo di studenti e personale, la gestione dell'accesso unico all'IT, l'accesso agli edifici, lo scambio Erasmus e altri processi di applicazione sono i casi d'uso che derivano dall'abilitazione delle parti interessate con credenziali verificabili.

Gli studenti e il personale possono beneficiare delle loro VC accademiche nella comunità più ampia. Ad esempio, possono usare il loro ID VC per accedere a sconti per studenti nei trasporti pubblici e nei servizi, nei negozi, nei ristoranti e nei luoghi di intrattenimento.

* Lavoro

Le carte VC per i dipendenti emesse dai datori di lavoro e altre VC rilasciate dalle amministrazioni pubbliche possono migliorare l'esperienza dei dipendenti e dei lavoratori durante i processi di onboarding, accesso agli edifici e accesso all'IT (portale dei dipendenti e altri sistemi aziendali).

Tuttavia, i vantaggi dell'esperienza utente nell'ecosistema lavorativo arrivano prima che l'utente venga assunto. I cittadini possono sfruttare i loro VC accademici e governativi per semplificare le domande di lavoro. Allo stesso tempo, i datori di lavoro limitano le frodi di identità.

* Commercio elettronico e vendita al dettaglio

Uno dei principali punti dolenti per gli utenti dei siti di e-commerce è tenere traccia di nomi utente e password. SSI li elimina completamente e si affida invece ai VC degli utenti per la verifica dell'identità, per fornire un'autenticazione e un onboarding istantanei e iper-sicuri.

I negozi di e-commerce e di vendita al dettaglio possono anche migliorare l'esperienza del cliente emettendo VC per tessere associative e di fidelizzazione, creando un percorso del cliente senza stress.

Allo stesso modo, nei mercati P2P, la tecnologia SSI aiuta a garantire che acquirenti e venditori siano quelli che dichiarano di essere e facilita le transazioni in modo semplice, sicuro e rispettoso della privacy.

* Semplificare il processo di reclutamento

Le organizzazioni che desiderano reclutare in modo efficiente candidati di alta qualità possono verificare istantaneamente con SSI le credenziali educative e professionali, come la laurea e i certificati professionali. Ciò consentirà di risparmiare giorni o settimane rispetto ai tradizionali processi di verifica manuale.

* Assistenza sanitaria

Per fornire un servizio efficiente e coerente, basato su informazioni accurate sull'identità e sulla storia medica di un paziente, SSI può aiutare a mantenere un registro accurato che può essere condiviso in modo efficiente con i fornitori di servizi sanitari pertinenti.

* Autenticazione di dipendenti e collaboratori

Le organizzazioni possono rilasciare credenziali verificabili per lo stato di dipendente o appaltatore. I titolari possono effettuare il login con il loro portafoglio di identità sovrana. Le organizzazioni possono aggiungere credenziali a scadenza per i collaboratori temporanei.

* Processi e compiti transfrontalieri

Tracciare le credenziali di spedizione e il loro utilizzo in modo semplice e veloce

* Conformità del cliente – Know Your Customer Compliance (KYC)

La conformità KYC può essere semplificata implementando le credenziali verificabili durante il processo di onboarding del cliente. Invece di eseguire un processo KYC diverso per ogni servizio sottoscritto, è possibile riutilizzare le credenziali KYC. Ad esempio, se l'azienda A ha eseguito un KYC e vi ha rilasciato credenziali verificabili, potete riutilizzare le stesse credenziali quando vi iscrivete all'azienda B per accelerare il processo KYC.

* NFT

SSI può aiutare a dimostrare chi ha creato, posseduto o possiede attualmente token non fungibili (NFT) durante il loro ciclo di vita. SSI può consentire a qualcuno di dimostrare di possedere un NFT senza dover collegare il proprio portafoglio ETH.

* Prova del reddito per i servizi finanziari e governativi

È possibile fornire una prova di reddito senza rivelare i propri guadagni totali.

* Voto per un'organizzazione come un club o un'azienda

SSI può essere utilizzato per garantire che solo i membri possano partecipare e votare. Le loro credenziali saranno collegate alla loro DID e i loro nomi non saranno rivelati. L'organizzazione può fidarsi che le persone siano chi dicono di essere e che abbiano il diritto di votare perché possono dimostrare crittograficamente di possedere il DID legittimo.

* Informazioni sull'immigrazione e demografiche

Le credenziali verificabili possono includere dettagli necessari per ottenere servizi governativi, come l'età avanzata, la condizione di veterano, di nativo/a aborigeno/a o di disabile. Le VC possono accelerare il processo di verifica, in quanto le persone possono utilizzare queste credenziali per richiedere un programma governativo o dimostrare qualcosa su di sé in modo rapido e senza tempi di attesa.

* Integrazione con protocolli esistenti

Protocolli ad accesso centralizzato come SAML, OAuth 2.0, OpenID Connect possono essere usati per garantire un alto LoA (Level of Assurance). Essi sono tutti protocolli di autenticazione e autorizzazione utilizzati per gestire l'accesso sicuro alle risorse digitali. Nello specifico:

* Security Assertion Markup Language (SAML): è un protocollo di autenticazione e autorizzazione che consente la condivisione di informazioni di autenticazione e autorizzazione tra due parti, come ad esempio un'organizzazione che fornisce un servizio e un utente che richiede l'accesso a quel servizio. In SAML, l'organizzazione che fornisce il servizio (noto come Service Provider o SP) richiede all'utente di autenticarsi tramite un'identità federata (noto come Identity Provider o IdP). L'IdP autentica l'utente e fornisce all'SP un token di autorizzazione che contiene informazioni sulle autorizzazioni dell'utente per accedere al servizio. Questo token è criptato e firmato digitalmente per garantirne la sicurezza.
* OAuth 2.0: è un protocollo di autorizzazione che consente a un utente di concedere a un'applicazione terza (noto come Client) l'accesso a una risorsa protetta da un'altra applicazione (noto come Resource Server), senza dover condividere le credenziali di autenticazione dell'utente. In OAuth 2.0, l'utente autorizza il Client ad accedere alle proprie informazioni personali sul Resource Server tramite un token di accesso. Questo token è valido solo per le autorizzazioni specifiche concesse dall'utente e ha una scadenza limitata.
* OpenID Connect: è un protocollo di autenticazione che utilizza OAuth 2.0 come base per fornire un'identità federata. In OpenID Connect, l'utente autentica l'Identity Provider (noto come OpenID Provider o OP) e quindi utilizza questo autenticazione per accedere alle risorse protette dal Service Provider (SP). In questo modo, l'utente può accedere a diversi servizi senza dover autenticarsi ripetutamente. OpenID Connect fornisce un token di identità che contiene informazioni sull'identità dell'utente, come ad esempio il nome e l'indirizzo e-mail. Questo token è criptato e firmato digitalmente per garantirne la sicurezza.
* Finanza decentralizzata (DeFi)

SSI condivide gli stessi principi di decentralizzazione della DeFi, il che la rende un partner ideale per la verifica dell'identità. SSI elimina la necessità di passare attraverso un processo di KYC o di registrazione per ogni dApp.

Il principale caso d'uso di SSI della DeFi è il KYC decentralizzato per le cripto/ICO e l'onboarding istantaneo, conforme e sicuro nelle piattaforme cripto/DeFi.

Allo stesso modo, gli exchange e le dApp della DeFi possono svolgere un ruolo di emittenti rilasciando credenziali KYC agli utenti che hanno superato il KYC. Idealmente, queste credenziali KYC sarebbero riutilizzabili e trasferibili a qualsiasi servizio di Web3.

* Telecomunicazioni

L'anno scorso, SK Telecom e Deutsche Telekom hanno annunciato l'intenzione di lanciare un progetto pilota di identificazione digitale che si baserà sulle capacità tecnologiche della blockchain per contribuire a semplificare la gestione del controllo degli accessi, dei contratti e di altri rapporti tra l'operatore e i suoi clienti.

Inoltre, SK Telecom ha grandi progetti nel suo mercato nazionale, la Corea del Sud. L'azienda sta pianificando di consentire a ogni abbonato di memorizzare la propria identità digitale e i propri dati personali, per poi utilizzare questi dati per fornire una soluzione di autenticazione alla sua crescente rete di partner, tra cui Samsung Electronics, KEB Hana Bank, Woori Bank e Koscom. L'ambito dei potenziali casi d'uso che la telecom sta sfruttando comprende:

* Certificazione dei documenti accademici e dei diplomi rilasciati dalle università coreane.
* Certificazione dei dati relativi a trattamenti e risarcimenti, che potrebbero essere forniti agli assicuratori su richiesta.
* Memorizzazione di pass per strutture di intrattenimento, resort e country club con ulteriori opportunità di marketing.

Samsung, che partecipa anch'essa all'iniziativa, ha promesso di garantire una memorizzazione sicura dei dati PII sul dispositivo con Samsung Knox, una soluzione di sicurezza mobile di livello aziendale, preinstallata sulla maggior parte dei dispositivi del marchio. A giugno 2020, l'azienda ha anche messo in vendita in Corea del Sud il suo primo modello di smartphone basato su blockchain, il KlaytnPhone. Il nuovo gadget è dotato di un portafoglio di criptovalute e di applicazioni di distributed ledger technology (DLT), costruite sulla blockchain di Klaytn.

Diventare un fornitore di soluzioni SSI è solo una delle strade che le telecomunicazioni possono percorrere quando si tratta di adottare la blockchain. I vantaggi di affidarsi a soluzioni SSI "fatte in casa" o di terzi nel settore delle telecomunicazioni si estendono ulteriormente:

* KYC remoto più rapido per i nuovi abbonati, soprattutto nei mercati in via di sviluppo, dove l'accesso a sedi fisse può essere limitato.
* Una migliore gestione dell'identità che consentirebbe agli abbonati esistenti di iscriversi a nuovi servizi da remoto e di gestire meglio i loro contratti.
* Un processo di autenticazione più forte può anche ridurre i livelli di frode vocale nel settore delle telecomunicazioni, grazie a una migliore tracciabilità degli abbonati e dei dispositivi.

## Protocolli

Ci sono diversi protocolli per la gestione delle identità digitali, o Digital Identity Management, utilizzati per garantire l'identificazione sicura e affidabile degli utenti nei contesti digitali. In particolare, gli utenti hanno il controllo completo sulle proprie informazioni di identità digitali e possiamo determinare protocolli di autorizzazione o di autenticazione forte (con l’ausilio di dispositivi fisici).

Citiamo la FIDO Alliance (Fast Identity Online), un'organizzazione internazionale composta da aziende leader nel settore della sicurezza informatica, che si occupa di sviluppare standard e protocolli per l'identità digitale e l'autenticazione sicura. L'obiettivo principale della FIDO Alliance è di creare un ecosistema di autenticazione sicura, interoperabile e user-friendly, basato su standard aperti e condivisi.

La FIDO Alliance ha sviluppato due principali standard di autenticazione: FIDO U2F e FIDO2.

* FIDO2, protocollo di autenticazione FIDO2 è un protocollo di autenticazione sviluppato dalla FIDO Alliance (Fast Identity Online) che consente di autenticare l'identità digitale degli utenti in modo sicuro, affidabile e rispettando la privacy delle informazioni personali. FIDO2 è basato sulla crittografia a chiave pubblica e può essere utilizzato per autenticare l'accesso a siti web, applicazioni e servizi online.
* Il protocollo FIDO2 è composto da due componenti principali: WebAuthn e CTAP (Client to Authenticator Protocol).
  + WebAuthn è un'API (Application Programming Interface) sviluppata dal W3C (World Wide Web Consortium) che consente ai siti web di utilizzare la crittografia a chiave pubblica per autenticare l'identità degli utenti. In pratica, WebAuthn consente agli utenti di utilizzare un dispositivo hardware o un'applicazione per autenticare la propria identità digitale senza dover condividere informazioni personali con il servizio online. WebAuthn è supportato da diversi browser web, tra cui Google Chrome, Firefox e Microsoft Edge.
  + CTAP (Client to Authenticator Protocol) è invece un protocollo di comunicazione sviluppato dalla FIDO Alliance che consente ai dispositivi hardware di comunicare con i client web. CTAP permette ai dispositivi hardware di inviare informazioni di autenticazione ai siti web in modo sicuro e affidabile, utilizzando la crittografia a chiave pubblica.
* In pratica, per autenticarsi utilizzando FIDO2, l'utente deve prima registrare il proprio dispositivo hardware o l'applicazione con il servizio online. Durante la registrazione, il servizio online genera una coppia di chiavi crittografiche: una chiave pubblica e una chiave privata. La chiave privata viene memorizzata sul dispositivo hardware o sull'applicazione, mentre la chiave pubblica viene inviata al servizio online.
* Quando l'utente accede al servizio online, il servizio richiede l'autenticazione utilizzando FIDO2. L'utente quindi utilizza il proprio dispositivo hardware o l'applicazione per generare una firma digitale utilizzando la propria chiave privata. La firma digitale viene inviata al servizio online, che utilizza la chiave pubblica per verificare l'autenticità della firma.
* Il protocollo FIDO2 offre diversi vantaggi rispetto ad altre forme di autenticazione, come ad esempio le password. In primo luogo, la crittografia a chiave pubblica consente di autenticare l'identità digitale degli utenti senza la necessità di condividere informazioni personali con il servizio online. Inoltre, l'uso di dispositivi hardware o applicazioni per autenticarsi garantisce una maggiore sicurezza rispetto alle password, che possono essere facilmente compromesse in caso di violazione dei dati.
* In sintesi, FIDO2 è un protocollo di autenticazione basato sulla crittografia a chiave pubblica che consente di autenticare l'identità digitale degli utenti in modo sicuro, affidabile e rispettando la privacy delle informazioni personali. FIDO2 è composto da due componenti principali: WebAuthn e CTAP, che consentono ai dispositivi hardware o alle applicazioni di comunicare in modo sicuro con i servizi online.
* FIDO U2F, che invece utilizza una chiave fisica per autenticare l'utente, garantendo una maggiore sicurezza rispetto alle password e altre forme di autenticazione.
  + Il funzionamento di FIDO U2F è abbastanza semplice. Innanzitutto, l'utente deve registrare la propria chiave fisica con il servizio online. Durante la registrazione, il servizio online genera una coppia di chiavi crittografiche: una chiave pubblica e una chiave privata. La chiave pubblica viene inviata al dispositivo hardware, mentre la chiave privata viene memorizzata sul servizio online.
  + Successivamente, quando l'utente accede al servizio online, il servizio richiede l'autenticazione utilizzando FIDO U2F. L'utente quindi inserisce la chiave fisica nel computer o nel dispositivo mobile e preme un pulsante per autenticarsi. La chiave fisica genera quindi una firma digitale utilizzando la chiave privata, che viene inviata al servizio online. Il servizio online utilizza la chiave pubblica per verificare l'autenticità della firma digitale e accedere all'account dell'utente.
  + La chiave fisica utilizzata da FIDO U2F è un dispositivo USB o NFC (Near Field Communication) che può essere facilmente trasportato con l'utente. La chiave fisica garantisce una maggiore sicurezza rispetto alle password, in quanto non può essere facilmente compromessa in caso di violazione dei dati. Inoltre, la chiave fisica può essere utilizzata per autenticarsi su diversi dispositivi e servizi online.
  + FIDO U2F offre diversi vantaggi rispetto ad altre forme di autenticazione. In primo luogo, la chiave fisica garantisce una maggiore sicurezza rispetto alle password e altre forme di autenticazione, poiché non può essere facilmente compromessa in caso di violazione dei dati. Inoltre, la chiave fisica può essere utilizzata per autenticarsi su diversi dispositivi e servizi online, garantendo una maggiore flessibilità e convenienza per l'utente.

La FIDO Alliance può essere utilizzata come riferimento per la Self Sovereign Identity (SSI) in quanto i suoi standard di autenticazione sono basati su principi di sicurezza, interoperabilità e privacy delle informazioni personali dell'utente, che sono anche fondamentali per la SSI. Inoltre, l'approccio della FIDO Alliance è simile a quello della SSI, poiché entrambi cercano di creare un ecosistema di autenticazione sicura e decentralizzata, basata su standard aperti e condivisi.

* Un altro protocollo interessante è OAuth, un protocollo di autorizzazione standardizzato e ampiamente utilizzato per consentire l'accesso limitato a risorse protette su Internet senza la necessità di condividere le credenziali di accesso dell'utente (username e password) funzionante tramite il protocollo HTTP.
  + In sostanza, OAuth consente a un'applicazione (chiamata client) di accedere alle risorse protette (come i dati dell'utente) su un server (chiamato resource server) in nome dell'utente, senza che l'applicazione debba conoscere le credenziali di accesso dell'utente. Invece, l'utente autorizza la richiesta di accesso dell'applicazione tramite un meccanismo di autorizzazione basato su token.
* Il processo di autorizzazione in OAuth prevede quattro attori principali:
  + L'utente (Resource Owner): l'utente che desidera concedere l'accesso alle proprie risorse protette.
  + Il client (o Consumer): l'applicazione che desidera accedere alle risorse protette dell'utente.
  + L'autorizzatore (Authorization Server): il server che gestisce l'autorizzazione dell'accesso alle risorse protette.
  + Il Resource Server (o Service Provider): il server che ospita le risorse protette.
* Il processo di autorizzazione in OAuth si svolge in tre fasi principali:
  + Autorizzazione: l'utente autorizza il client ad accedere alle proprie risorse protette.
  + Concessione dell'accesso: il server di autorizzazione concede l'accesso al client e fornisce un token di accesso.
  + Accesso alle risorse: il client utilizza il token di accesso per accedere alle risorse protette sul resource server.
* Il token di accesso in OAuth può essere di due tipi: token di accesso a breve termine (access token) e token di aggiornamento (refresh token). Il token di accesso a breve termine è utilizzato dal client per accedere alle risorse protette per un periodo limitato di tempo (solitamente poche ore), mentre il token di aggiornamento può essere utilizzato dal client per ottenere un nuovo token di accesso quando quello precedente è scaduto.

L’idea alla base è di consentire l’accesso alle risorse protette senza condividere alcuna credenziale, ma anzi migliorando l’esperienza dell’utente e consentire l’accesso a risorse protette su vari siti web. Di questo protocollo esistono due versioni: 1.0 e 2.0.

* La versione 1.0 di OAuth presentava alcune limitazioni, come la mancanza di standardizzazione e la complessità del processo di autorizzazione. Inoltre, la versione 1.0 non forniva un meccanismo per la revoca del token di accesso in caso di violazione della sicurezza.
  + Di fatto, inoltre, il processo di autorizzazione prevede la firma digitale di tutte le richieste, il che può essere un processo complesso da gestire.
* Per superare queste limitazioni, è stata sviluppata la versione 2.0 di OAuth. La versione 2.0 di OAuth è stata semplificata e standardizzata dall’IETF, e include nuove funzionalità come la revoca del token di accesso e il supporto per la firma digitale dei token.

OAuth 2.0 è stato progettato per supportare scenari di autenticazione e autorizzazione più complessi rispetto al suo predecessore, OAuth 1.0. Ecco alcuni modi in cui OAuth 2.0 raggiunge questo obiettivo:

* Separazione dei ruoli: OAuth 2.0 separa i ruoli del server di autorizzazione e del server delle risorse. Il server di autorizzazione è responsabile della concessione dei token di accesso ai client, mentre il server delle risorse è responsabile della verifica dei token di accesso e dell'accesso alle risorse protette. Questa separazione dei ruoli consente scenari di autorizzazione più complessi, in quanto il server di autorizzazione può concedere diversi tipi di token di accesso a diversi client e il server delle risorse può applicare politiche di controllo dell'accesso a grana fine in base al tipo di token di accesso.
* Supporto per diversi tipi di concessione: OAuth 2.0 supporta diversi tipi di concessione, che vengono utilizzati per ottenere token di accesso per diversi scenari. Ad esempio, il tipo di concessione del codice di autorizzazione viene utilizzato quando il client è un'applicazione web che può memorizzare in modo sicuro il segreto del client, mentre il tipo di concessione delle credenziali del client viene utilizzato quando il client è un client riservato che può autenticarsi con il server di autorizzazione.
* Registrazione dinamica del client: OAuth 2.0 permette ai client di registrarsi dinamicamente con il server di autorizzazione, consentendo scenari di autenticazione e autorizzazione più flessibili. Ad esempio, un client può registrarsi presso il server di autorizzazione e ottenere un ID e un segreto del client, che possono essere utilizzati per autenticare il client durante il flusso di autorizzazione.
* Integrazione con OpenID Connect: OAuth 2.0 può essere integrato con OpenID Connect, un protocollo di autenticazione che consente ai client di ottenere informazioni sull'identità dell'utente finale. OpenID Connect si basa su OAuth 2.0 e aggiunge ulteriori funzionalità, come i token ID, che contengono informazioni sull'identità dell'utente.

Esaminiamo pro e contro di OpenID:

* Per pro, OAuth utilizza il protocollo HTTPS per garantire la sicurezza delle informazioni di autenticazione degli utenti durante il processo di autorizzazione. Inoltre, semplifica il processo di accesso ai servizi web, eliminando la necessità di creare e gestire molteplici account. Inoltre, è scalabile e può essere utilizzato da ogni servizio web o applicazione
* Per contro, oltre ai protocolli e all’implementazione, i servizi web che utilizzano OAuth dipendono dal provider di identità per l'autenticazione degli utenti. Se il provider di identità diventa inattivo o viene violato, gli utenti possono essere bloccati dall'accesso ai servizi web che utilizzano OAuth. Inoltre, in alcuni casi, una volta che un utente ha concesso l'autorizzazione a un'applicazione tramite OAuth, l'autorizzazione non può essere revocata. Ciò significa che l'applicazione continua ad avere accesso alle risorse dell'utente senza il consenso dell'utente stesso.

Essendo stato citato più volte, parliamo ora di OpenID Connect (OIDC), che è un protocollo di autenticazione costruito sulla base di OAuth 2.0. Fornisce un modo standardizzato per i client di ottenere informazioni sull'identità dell'utente finale e consente il single sign-on (SSO) tra più applicazioni e domini.

* OIDC definisce tre parti principali: il client, il provider OpenID (OP) e l'utente finale. Il client è l'applicazione che vuole autenticare l'utente finale, l'OP è il server che autentica l'utente finale e fornisce le informazioni sull'identità e l'utente finale è la persona che viene autenticata.
* Il flusso di autenticazione OIDC consiste nelle seguenti fasi:
  + Il client avvia il flusso di autenticazione reindirizzando l'utente finale all'endpoint di autorizzazione dell'OP con una richiesta di autenticazione.
  + L'OP verifica l'identità dell'utente finale e ottiene il consenso per l'accesso richiesto dall'utente finale.
  + L'OP genera un token ID, che contiene informazioni sull'identità dell'utente finale, e lo restituisce al cliente.
  + Il client può quindi utilizzare il token ID per autenticare l'utente finale e ottenere ulteriori informazioni sulla sua identità, come il nome e l'indirizzo e-mail.
* OIDC supporta diverse funzionalità che lo rendono un protocollo di autenticazione potente:
  + Single sign-on (SSO): OIDC consente l'SSO tra più applicazioni e domini. Una volta che l'utente finale si è autenticato con l’OP, può accedere ad altre applicazioni che supportano OIDC senza doversi autenticare nuovamente.
  + Informazioni standardizzate sull'identità: OIDC definisce un insieme standardizzato di informazioni che possono essere incluse nel token ID, come il nome dell'utente, l'indirizzo e-mail e la lingua preferita. In questo modo è più facile per i client ottenere informazioni sull'identità dal token ID senza dover effettuare richieste API aggiuntive.
  + Integrazione con OAuth 2.0: OIDC è costruito sulla base di OAuth 2.0 e utilizza gli stessi flussi di autorizzazione. Questo rende facile per i clienti integrare OIDC nei loro flussi di autenticazione OAuth 2.0 esistenti.
  + Federazione: OIDC supporta la federazione, che consente a più OP di lavorare insieme per autenticare gli utenti finali. Ciò consente l'SSO tra più domini e organizzazioni.

Esaminiamo pro e contro di OpenID:

* Possiamo descrivere una maggiore convenienza, in quanto OpenID elimina la necessità di creare e gestire molteplici account in diversi siti web. Inoltre, utilizza la crittografia a chiave pubblica e gli utenti possono scegliere di condividere solo le informazioni necessarie per accedere al sito web e possono revocare l'accesso in qualsiasi momento. Si noti poi che è un protocollo aperto che può essere utilizzato da qualsiasi sito web o provider di identità.
* Tuttavia, se l'account OpenID viene compromesso, l'accesso a tutti i siti web che utilizzano OpenID può essere compromesso. Inoltre, gli utenti dipendono dal provider di identità per l'accesso ai siti web che utilizzano OpenID. Se il provider di identità diventa inattivo o viene violato, gli utenti potrebbero non essere in grado di accedere ai siti web che utilizzano OpenID. Inoltre, per i vari protocolli che supporta, può essere complesso da implementare nei singoli siti in cui è presente.

Riguardo al Single Sign-On (SSO), possiamo citare SAML (Security Assertion Markup Language) è un protocollo standard per l'autenticazione e l'autorizzazione degli utenti in un ambiente di accesso singolo (Single Sign-On, SSO). SAML consente agli utenti di autenticarsi una sola volta su un servizio web e di accedere a più servizi web senza dover inserire nuovamente le proprie credenziali di accesso.

SAML utilizza una combinazione di protocolli XML per consentire agli utenti di autenticarsi e autorizzare l'accesso a risorse protette. In particolare, SAML utilizza tre componenti principali:

* Identity Provider (IDP): il provider di identità è il sistema che gestisce le informazioni di autenticazione degli utenti e fornisce l'accesso alle risorse protette ai servizi web.
* Service Provider (SP): il fornitore di servizi è il sistema che fornisce l'accesso alle risorse protette ai propri utenti e si affida al provider di identità per gestire l'autenticazione degli utenti.
* User: l'utente è la persona che accede ai servizi web protetti e che deve autenticarsi tramite il provider di identità.

Viene usato un particolare documento in fase di autenticazione, definito come SAML Assertion, documento XML che il fornitore di identità invia al fornitore di servizi e che contiene l'autorizzazione dell'utente. Esistono tre diversi tipi di asserzioni SAML: autenticazione, attributo e decisione di autorizzazione.

* Le asserzioni di autenticazione dimostrano l'identificazione dell'utente e forniscono l'ora in cui l'utente ha effettuato l'accesso e il metodo di autenticazione utilizzato (ad esempio, Kerberos, 2 fattori, ecc.).
* L'asserzione di attribuzione passa gli attributi SAML al fornitore di servizi - gli attributi SAML sono dati specifici che forniscono informazioni sull'utente.
* Un'asserzione di decisione di autorizzazione dice se l'utente è autorizzato a usare il servizio o se il fornitore di identificazione ha negato la sua richiesta a causa di un errore nella password o della mancanza di diritti al servizio.

Il processo di autenticazione di SAML funziona nel seguente modo:

* L'utente tenta di accedere a un servizio web protetto.
* Il servizio web redirige l'utente al provider di identità per l'autenticazione.
* Il provider di identità richiede all'utente di inserire le proprie credenziali di accesso.
* Se le credenziali di accesso sono valide, il provider di identità genera un Assertion (un documento XML firmato digitalmente) che contiene le informazioni di autenticazione dell'utente.
* Il provider di identità invia l'Assertion al servizio web.
* Il servizio web verifica l'Assertion e autorizza l'accesso dell'utente alle risorse protette.

Come per i precedenti, a livello di pro e contro:

* Usa HTTPS, risulta essere interoperabile tra sistemi ed applicazioni, consente agli utenti di mantenere il controllo delle proprie informazioni e risulta scalabile. Risulta uno standard aperto
* Anche qui, comunque si dipende dal provider di identità, non tutti i servizi supportano SAML e utilizza XML come linguaggio di markup. Inoltre, l’eliminazione dei dati, per un impiegato, deve essere fatta dall’amministrazione.

Citiamo anche SCIM (System for Cross-domain Identity Management) è uno standard aperto per la gestione delle identità digitali e delle autorizzazioni degli utenti in ambienti cloud e multi-domain. SCIM consente di semplificare la gestione delle identità digitali e delle autorizzazioni degli utenti in un ambiente distribuito, consentendo di creare, modificare e rimuovere le informazioni di identità degli utenti in modo efficiente e sicuro.

SCIM utilizza un protocollo RESTful basato su JSON per consentire l'integrazione tra i diversi sistemi e le diverse applicazioni che gestiscono le identità digitali degli utenti. In particolare, SCIM definisce due componenti principali:

* Service Provider (SP): il fornitore di servizi è il sistema che gestisce le informazioni di identità degli utenti e fornisce l'accesso ai servizi alle applicazioni e ai servizi web.
* Identity Provider (IDP): il provider di identità è il sistema che gestisce le informazioni di autenticazione degli utenti e fornisce l'autenticazione ai servizi web e alle applicazioni.

Il processo di gestione delle identità in SCIM funziona nel seguente modo:

* L'IDP crea o aggiorna le informazioni di identità dell'utente.
* L'IDP invia le informazioni di identità all'SP tramite una richiesta RESTful.
* L'SP elabora le informazioni di identità e le memorizza nel proprio database.
* L'SP invia una conferma di successo all'IDP.
* L'IDP notifica l'utente del successo dell'operazione.

In questo modo, SCIM consente di mantenere la coerenza delle informazioni di identità degli utenti tra i diversi sistemi e applicazioni, semplificando la gestione delle autorizzazioni e migliorando la sicurezza delle informazioni di identità.

SCIM può essere utilizzato in diversi contesti, tra cui l'accesso alle applicazioni cloud, la gestione delle autorizzazioni degli utenti e la gestione delle identità degli utenti in ambienti multi-domain. Inoltre, SCIM può essere integrato con altri protocolli di autenticazione, come SAML, OAuth e OpenID Connect, per fornire una soluzione completa di gestione delle identità digitali e delle autorizzazioni degli utenti.

## Casi d’uso reali

Nella successiva sezione, esamineremo Individuare casi d’uso reali per la SSI, analizzando i consorzi internazionali coinvolti in ambito di ricerca e i finanziamenti europei.

* DECODE (Decentralized Citizen Owned Data Ecosystem), progetto europeo che mira a creare un'infrastruttura di dati decentralizzata e sicura per i cittadini europei. Il progetto utilizza tecnologie blockchain e Self-Sovereign Identity (SSI) per consentire ai cittadini di controllare le proprie informazioni personali e condividerle solo con le parti autorizzate.
  + Esso è stato avviato nel 2017 e ha ricevuto finanziamenti dal programma europeo Horizon 2020. Il progetto coinvolge un consorzio di organizzazioni provenienti da diversi paesi europei, tra cui università, centri di ricerca, organizzazioni non-profit e aziende private.
  + In particolare, DECODE utilizza una blockchain pubblica basata su Ethereum per creare un registro distribuito delle informazioni personali degli utenti. Le informazioni personali sono crittografate e protette da meccanismi di sicurezza avanzati, tra cui la crittografia a chiave pubblica, per garantire la privacy e la sicurezza degli utenti.
  + Inoltre, DECODE utilizza tecnologie SSI per consentire agli utenti di controllare le proprie informazioni di identità digitale e di condividerle solo con le parti autorizzate. In pratica, ogni utente ha una chiave privata unica che utilizza per firmare digitalmente le proprie informazioni di identità e condividerle con le parti autorizzate. Questo consente agli utenti di controllare le proprie informazioni di identità e di evitare la divulgazione non autorizzata delle loro informazioni personali.
  + L'obiettivo principale di DECODE è creare un'infrastruttura di dati decentralizzata che sia controllata e di proprietà dei cittadini europei. L'infrastruttura consentirà ai cittadini di archiviare le proprie informazioni personali in modo sicuro e di condividerle solo con le parti autorizzate. Inoltre, DECODE mira a creare un ecosistema di applicazioni e servizi basati sui dati che siano trasparenti, equi e rispettosi della privacy degli utenti.
* DECODE ha sviluppato anche una serie di applicazioni e servizi basati sui dati che utilizzano l'infrastruttura di dati decentralizzata del progetto. Ad esempio, il progetto ha sviluppato un'applicazione per il monitoraggio della qualità dell'aria basata sui dati raccolti dai sensori ambientali. L'applicazione consente agli utenti di monitorare la qualità dell'aria nella propria zona e di condividere le informazioni con le autorità locali per migliorare la qualità dell'aria.
* IDunion, che è un consorzio tedesco che mira a creare un'infrastruttura di identità digitale basata sulla tecnologia Self-Sovereign Identity (SSI). Il progetto è stato avviato nel 2019 e coinvolge diverse organizzazioni tedesche, tra cui università, istituti di ricerca, privati e organizzazioni non-profit.
  + L'obiettivo principale di IDunion è creare un'infrastruttura di identità digitale che consenta agli utenti di controllare le proprie informazioni personali e di condividerle solo con le parti autorizzate. La tecnologia SSI consente agli utenti di avere un controllo completo sulle proprie informazioni di identità digitale, senza dover affidarsi a terze parti centralizzate.
  + Per raggiungere questi obiettivi, IDunion utilizza una blockchain privata basata su Hyperledger Indy per creare un registro distribuito delle informazioni di identità digitale degli utenti. Le informazioni sono crittografate e protette da meccanismi di sicurezza avanzati per garantire la privacy e la sicurezza degli utenti.
  + Inoltre, ogni utente ha la possibilità di creare un registro personale di identità digitali (DID), che funge da identificatore univoco dell'utente sulla blockchain. Il registro DID è associato alla chiave privata dell'utente e consente all'utente di controllare completamente le proprie informazioni di identità digitale.
* IRMA (I Reveal My Attributes), un sistema di identità digitale basato sulla tecnologia SSI (Self-Sovereign Identity) sviluppato dall'Università di Twente e da una serie di partner in Europa. Il progetto IRMA mira a sviluppare un sistema di identità digitale decentralizzato, sicuro e rispettoso della privacy che consenta agli utenti di controllare completamente le proprie informazioni di identità digitale.
  + Esso si basa sulla tecnologia di Zero Knowledge Proof (ZKP) per consentire agli utenti di dimostrare di possedere determinate informazioni di identità senza doverle rivelare effettivamente. In questo modo, gli utenti possono utilizzare le proprie informazioni di identità in modo selettivo e in modo rispettoso della privacy.
  + Il sistema utilizza una combinazione di tecnologie basate su blockchain e crittografia per garantire la sicurezza e la privacy dei dati di identità degli utenti. In particolare, il sistema utilizza una blockchain privata per la gestione delle identità digitali degli utenti e la crittografia end-to-end per garantire la privacy durante la trasmissione dei dati di identità.
* Il sistema IRMA utilizza un'applicazione mobile che funge da portafoglio digitale per le informazioni di identità dell'utente. L'applicazione utilizza la crittografia end-to-end per garantire la privacy delle informazioni di identità durante la trasmissione.
  + Il sistema IRMA utilizza anche una tecnologia di crittografia avanzata chiamata Attribute-Based Encryption (ABE) per garantire la sicurezza delle informazioni di identità degli utenti. L'ABE consente di crittografare i dati di identità in modo selettivo, in base agli attributi dell'utente. In questo modo, solo le persone che soddisfano determinati requisiti di attributi possono accedere alle informazioni di identità.
  + Una volta che un utente desidera utilizzare le proprie informazioni di identità, l'applicazione mobile IRMA genera una prova crittografica che dimostra che l'utente possiede determinate informazioni di identità, senza doverle rivelare effettivamente. La prova crittografica viene quindi presentata all'organizzazione che richiede l'accesso alle informazioni di identità.
  + L'organizzazione può quindi verificare la prova crittografica utilizzando una chiave pubblica associata all'utente. La verifica della prova crittografica consente all'organizzazione di accedere solo alle informazioni di identità necessarie per la transazione, senza dover accedere a tutte le informazioni di identità dell'utente.
* Questo è stato utilizzato in diversi casi d'uso reali, tra cui la verifica dell'età per l'acquisto di alcolici e tabacco in Olanda, la verifica dell'identità per l'accesso ai servizi medici in Norvegia e la verifica dell'identità per l'accesso ai servizi pubblici in Estonia.
  + Il progetto IRMA è stato sviluppato da un consorzio di partner in Europa, tra cui università, istituti di ricerca e aziende private. Il progetto è stato finanziato in parte dalla Commissione Europea attraverso il programma Horizon 2020, che ha fornito un finanziamento di 5,6 milioni di euro per lo sviluppo del progetto.
* DIF (Decentralized Identity Foundation - DIF), consorzio internazionale senza scopo di lucro che si occupa della promozione e dello sviluppo di tecnologie di identità digitale decentralizzate basate sulla tecnologia SSI (Self-Sovereign Identity). La DIF è composta da un gruppo di aziende, organizzazioni e individui impegnati a promuovere l'adozione di tecnologie di identità digitale decentralizzate.
  + La missione della DIF è di sviluppare standard e protocolli aperti per la tecnologia SSI, al fine di consentire agli utenti di controllare completamente le proprie informazioni di identità digitali e di utilizzarle in modo sicuro e rispettoso della privacy.
* La DIF ha sviluppato diversi progetti e tecnologie per la realizzazione della sua missione, tra cui:
  + Universal Resolver: un sistema di risoluzione degli identificatori decentralizzato che consente di identificare le risorse su diverse reti blockchain e di identità decentralizzate.
    - Esso utilizza un protocollo standardizzato per la risoluzione degli identificatori, che consente di identificare in modo univoco una risorsa sulla rete.
    - Il sistema Universal Resolver è costituito da un insieme di server che forniscono un'interfaccia comune per la risoluzione degli identificatori. Ogni server è configurato per risolvere gli identificatori su una particolare rete blockchain o di identità decentralizzata.
    - Di fatto, funziona in modo simile al sistema Domain Name System (DNS) utilizzato per risolvere i nomi di dominio su Internet. Tuttavia, mentre il sistema DNS si basa su un'infrastruttura centralizzata, il sistema Universal Resolver è completamente decentralizzato e non dipende da un'autorità centrale.
  + Verifiable Credentials: un protocollo per la creazione, lo scambio e la verifica di credenziali verificabili basate sulla tecnologia SSI.
    - Il protocollo Verifiable Credentials consente agli utenti di creare credenziali verificabili utilizzando le proprie informazioni di identità digitali. Le credenziali verificabili possono essere utilizzate per l'accesso a servizi e risorse online senza dover rivelare le proprie informazioni di identità effettive.
    - In particolare, a livello standard viene stabilito un formato dalla W3C contenente una serie di dati che, una volta verificati e approvati correttamente dal funzionamento intrinseco del meccanismo SSI, garantisce la loro sostituzione a credenziali tradizionali, in quanto verificato in modo immutabile dal sistema blockchain.
  + Identity Hubs: un'architettura per la gestione delle identità digitali decentralizzate che consente agli utenti di controllare completamente le proprie informazioni di identità e di consentire l'accesso alle informazioni solo alle parti autorizzate.
    - In Identity Hubs, l'utente possiede un hub di identità digitale che contiene le proprie informazioni di identità. L'hub di identità digitale è completamente controllato dall'utente e può essere utilizzato per gestire le proprie informazioni di identità in modo selettivo e rispettoso della privacy.
    - L'architettura Identity Hubs utilizza un sistema di crittografia simmetrica per garantire la sicurezza delle informazioni di identità dell'utente. Le informazioni di identità sono crittografate in modo selettivo in base agli attributi dell'utente e possono essere visualizzate solo dalle parti autorizzate. Di fatto, utilizzano delle API di comunicazioni essendo delle tecnologie off-chain, comunicando tramite una serie di permessi con DID
* MyData, iniziativa internazionale volta a promuovere la gestione dei dati personale dell'utente, basata sui principi di autonomia, trasparenza e fiducia. Il progetto stato sviluppato inizialmente in Finlandia come iniziativa della Fondazione finlandese per l'innovazione Tekes, ma è diventato un'iniziativa globale che coinvolge diverse organizzazioni e consorzi internazionali.
  + L'iniziativa MyData ha sviluppato progetti e tecnologie per la realizzazione dela sua missione, tra cui:
    - MyData Operator: un'infrastruttura di dati personali decentralizzata che consente agli utenti di controllare le proprie informazioni personali e di gestirle in modo sicuro e rispettoso della privacy. Questa fornisce agli utenti un'interfaccia utente intuitiva per gestire le proprie informazioni personali e consentire l'accesso alle informazioni solo alle parti autorizzate. Le informazioni personali degli utenti sono crittografate in modo selettivo in base agli attributi dell'utente e possono essere visualizzate solo dalle parti autorizzate.
    - MyData Global Network: una rete globale di organizzazioni e individui che lavorano insieme per promuovere la gestione dei dati personali basata sui principi di MyData. La rete fornisce un forum per la condivisione delle migliori pratiche, delle conoscenze e delle esperienze tra i membri della rete. Inoltre, collabora con diverse organizzazioni e consorzi internazionali per promuovere la gestione dei dati personali.
    - MyData Commons: una piattaforma per la condivisione e la collaborazione sui dati personali tra gli utenti, le organizzazioni e le comunità.
* Kiva Protocol, un progetto a sé stante sviluppato in collaborazione con la Decentralized Identity Foundation (DIF) che utilizza la tecnologia SSI (Self-Sovereign Identity) per creare un'identità digitale sicura e rispettosa della privacy per le popolazioni svantaggiate in tutto il mondo.
  + L'obiettivo del Kiva Protocol è di fornire una soluzione di identità digitale sicura e rispettosa della privacy per le persone che non hanno accesso ai documenti di identità ufficiali, in modo che possano accedere a servizi finanziari, sanitari e sociali essenziali. Il Kiva Protocol si basa sui principi di MyData, ovvero autonomia, trasparenza e fiducia.
  + Il Kiva Protocol utilizza la tecnologia SSI per consentire alle persone di creare un'identità digitale unica e sicura. Prevede un processo di verifica dell'identità che coinvolge l'acquisizione di dati biometrici e personali dell'utente (eKYC). Il processo di verifica dell'identità è svolto da organizzazioni partner del Kiva Protocol, come le organizzazioni non governative (ONG) e le istituzioni finanziarie.
  + Una volta verificati, i dati di identità dell'utente vengono crittografati e memorizzati sulla blockchain. L'utente può quindi utilizzare la propria identità digitale per accedere ai servizi finanziari, sanitari e sociali di cui ha bisogno.
  + Il Kiva Protocol utilizza la blockchain per garantire la sicurezza e la privacy delle informazioni di identità degli utenti. La blockchain consente di mantenere un registro immutabile di tutte le transazioni, garantendo la sicurezza e la privacy delle informazioni. Infatti, si appoggia ad una piattaforma che offre servizi finanziari nota proprio come Kiva, garantendo dei prestiti sicuri e consentire agli utenti di accedere a servizi finanziari, come i prestiti, tramite FSP (Financial Service Provider).
* Sovrin Protocol, sottostante al framework Sovrin per l'identità digitale decentralizzata.
  + Utilizza una rete di nodi di consenso per registrare e verificare le informazioni di identità degli utenti sulla blockchain. La rete di nodi di consenso è gestita da un insieme di organizzazioni chiamate Sovrin Stewards. I Sovrin Stewards sono responsabili della governance della rete di nodi di consenso e della gestione della blockchain.
  + Inoltre, utilizza un sistema di token chiamato Sovrin Token per incentivare la partecipazione dei nodi di consenso alla rete. I nodi di consenso che partecipano alla rete ricevono una ricompensa in Sovrin Token per ogni blocco della blockchain validato.
  + Il Sovrin Protocol utilizza anche un sistema di firma digitale per garantire la sicurezza e l'autenticità delle informazioni di identità degli utenti. Il sistema di firma digitale utilizza la crittografia a chiave pubblica per garantire che solo l'utente possa accedere alle proprie informazioni di identità.
  + Incorporando il principio di privacy-by-default, vengono supportati DID (Decentralized Identifiers) e chiavi pubbliche uniche per ogni coppia di utenti. Nessun dato privato viene memorizzato sulla blockchain, nemmeno in forma cifrata, per prevenire la correlazione tra le informazioni di identità degli utenti. Inoltre, utilizza le zero-knowledge proofs per dimostrare la veridicità di una dichiarazione senza dover rivelare la dichiarazione stessa.
* ESSIF-Lab (European Self-Sovereign Identity Framework Laboratory), che è un progetto finanziato dall'Unione Europea che si occupa di promuovere e sviluppare l'adozione della tecnologia SSI (Self-Sovereign Identity) in Europa. Il progetto è coordinato dalla Commissione Europea e coinvolge diverse organizzazioni internazionali per la ricerca e lo sviluppo della tecnologia SSI.
  + L'architettura del framework di interoperabilità di ESSIF-Lab si basa su un insieme di componenti software che collaborano tra di loro per garantire la sicurezza e la privacy delle informazioni di identità degli utenti. Le componenti software principali del framework di interoperabilità di ESSIF-Lab includono:
    - Il DID Resolver: un componente software che consente agli utenti di risolvere i DIDs e di accedere alle informazioni di identità associate.
    - Il Verifiable Credentials Issuer: un componente software che consente agli utenti di creare attestazioni verificabili sulle proprie informazioni di identità.
    - Il Verifiable Credentials Holder: un componente software che consente agli utenti di gestire le attestazioni verificabili sulle proprie informazioni di identità.
    - Il Verifiable Credentials Verifier: un componente software che consente ai servizi online di verificare l'autenticità delle attestazioni verificabili sulle informazioni di identità degli utenti.

# Zero Knowledge Proof

Altri riferimenti matematici: <https://en.wikipedia.org/wiki/Zero-knowledge_proof>

Ad alto livello, una prova a conoscenza zero (zero-knowledge proof) funziona chiedendo al verificatore di eseguire una serie di azioni che possono essere eseguite con precisione solo se il verificatore conosce le informazioni sottostanti. Se il verificatore tira a indovinare il risultato di queste azioni, il test del verificatore gli darà torto con un alto grado di probabilità. Gli algoritmi Zero-Knowledge Proof (ZKP) sono algoritmi crittografici che calcolano la probabilità che una parte di una transazione possieda un'informazione senza dover rivelare quale sia tale informazione.

Le prove a conoscenza zero sono state descritte per la prima volta in un articolo del MIT del 1985 di Shafi Goldwasser e Silvio Micali, intitolato "The Knowledge Complexity of Interactive Proof-Systems". In questo documento, gli autori dimostrano che è possibile per un *prover* convincere un *verifier* che una specifica affermazione su un punto di dati è vera senza rivelare alcuna informazione aggiuntiva sui dati.

Le ZKP possono essere:

* interattive (Interactive Proofs), dove un *prover* convince un *verifier* specifico ma deve ripetere il processo per ogni singolo verificatore;
* non interattive (Non interactive Proofs), dove un *prover* genera una prova che può essere verificata da chiunque utilizzi la stessa prova e non richiedono transazione tra le parti che eseguono le transazioni oppure il processo di verifica prende luogo in una fase successiva.

Pur essendo rivoluzionaria, le interactive proofs avevano un'utilità limitata, poiché richiedevano che le due parti fossero disponibili e interagissero ripetutamente. Anche se un verificatore era convinto dell'onestà di un prover, la prova non sarebbe stata disponibile per una verifica indipendente (il calcolo di una nuova prova richiedeva una nuova serie di messaggi tra il prover e il verificatore).

Per risolvere questo problema, Manuel Blum, Paul Feldman e Silvio Micali hanno proposto le prime non interactive proofs a conoscenza zero in cui il prover e il verificatore hanno una chiave condivisa. Questo permette al prover di dimostrare la conoscenza di alcune informazioni (cioè il testimone) senza fornire le informazioni stesse.

A differenza delle prove interattive, le prove non interattive richiedono un solo ciclo di comunicazione tra i partecipanti (prover e verificatore). Il prover passa le informazioni segrete a uno speciale algoritmo per calcolare una prova a conoscenza zero. Questa prova viene inviata al verificatore, che controlla che il prover conosca le informazioni segrete utilizzando un altro algoritmo.

La prova non interattiva riduce la comunicazione tra prover e verificatore, rendendo le prove ZK più efficienti. Inoltre, una volta generata, la prova è disponibile per chiunque altro (con accesso alla chiave condivisa e all'algoritmo di verifica).

Le tre caratteristiche fondamentali che definiscono una ZKP sono:

* Completezza (Completeness): Se un'affermazione è vera, allora un verificatore onesto può essere convinto da un prover onesto di possedere la conoscenza dell'input corretto.
* Solidità (Soundness): Se un'affermazione è falsa, nessun prover disonesto può convincere unilateralmente un verificatore onesto di possedere la conoscenza dell'input corretto.
* Conoscenza zero (Zero-knowledge): Se lo stato è vero, il verificatore non apprende altro dal prover se non che l'affermazione è vera.

Di base, una ZKP è composta da tre elementi: testimone, sfida e risposta.

* Testimone (Witness): In una prova a conoscenza zero, il prover vuole dimostrare la conoscenza di alcune informazioni nascoste. L'informazione segreta è il "testimone" della prova e la presunta conoscenza del testimone da parte del prover stabilisce un insieme di domande a cui può rispondere solo chi conosce l'informazione. Pertanto, il prover inizia il processo di dimostrazione scegliendo a caso una domanda, calcolando la risposta e inviandola al verificatore.
* Sfida (Challenge): il verificatore sceglie a caso un'altra domanda dall'insieme e chiede al prover di rispondere.
* Risposta (Response): Il prover accetta la domanda, calcola la risposta e la restituisce al verificatore. La risposta del prover permette al verificatore di controllare se il primo ha davvero accesso al testimone. Per assicurarsi che il prover non stia indovinando alla cieca e non ottenga le risposte corrette per caso, il verificatore sceglie altre domande da porre. Ripetendo questa interazione più volte, la possibilità che il prover finga di conoscere il testimone diminuisce in modo significativo, finché il verificatore non è soddisfatto.

## Esempi

La caverna di Ali Babà è un esempio molto noto e utilizzato per spiegare le prove a conoscenza zero. In questo scenario, Peggy e Victor stanno esplorando una grotta con una porta segreta che può essere aperta solo pronunciando una password. Peggy conosce la password, ma Victor no.

* Per dimostrare a Victor che lei conosce la password, Peggy propone una prova a conoscenza zero. Propone che entrino nella grotta separatamente e che lei apra la porta segreta usando la password. Peggy tornerà poi fuori dalla grotta e aspetterà che Victor entri nella grotta e cerchi di aprire la porta. Se Victor riuscirà ad aprire la porta, potrà essere certo che Peggy conosce la parola d'ordine senza che lei debba mai rivelargliela.
* Tuttavia, Victor non è ancora del tutto convinto che Peggy conosca la password. Si preoccupa che Peggy possa averlo semplicemente osservato mentre digitava la password e che ora stia fingendo di aprire la porta usando le sue conoscenze. Per rispondere a questa preoccupazione, Peggy suggerisce di ripetere il processo più volte, con Victor che sceglie ogni volta una nuova password.
* Dopo diversi tentativi riusciti, Victor si convince che Peggy conosce davvero la password. La prova a conoscenza zero ha permesso a Peggy di dimostrare la sua conoscenza senza mai rivelare la password a Victor.

Questo esempio illustra come le prove a conoscenza zero possano essere utilizzate per stabilire la fiducia tra due parti senza rivelare alcuna informazione sensibile. In questo caso, Peggy è riuscita a convincere Victor di conoscere la password senza mai rivelare quale fosse la password.

## Tipi

Esistono diverse implementazioni di ZKP, ognuna delle quali presenta un proprio compromesso in termini di dimensione della prova, tempo del prover, tempo di verifica e altro ancora. Esse comprendono:

* zk-SNARK

Gli SNARK, acronimo di "succinct non-interactive argument of knowledge", sono di piccole dimensioni e facili da verificare. Generano una prova crittografica utilizzando le curve ellittiche, che sono più efficienti in termini di gas rispetto al metodo delle funzioni di hashing utilizzato da STARKS.

Il protocollo ZK-SNARK ha le seguenti qualità:

* Conoscenza zero (Zero-knowledge): Un verificatore può convalidare l'integrità di un'affermazione senza conoscere nient'altro dell'affermazione stessa. L'unica conoscenza che il verificatore ha dell'affermazione è se è vera o falsa.
* Succinta (Succint): la prova a conoscenza zero è più piccola del testimone e può essere verificata rapidamente.
* Non interattiva (Non interactive): La prova è "non interattiva" perché il prover e il verificatore interagiscono una sola volta, a differenza delle prove interattive che richiedono più cicli di comunicazione.
* Argomentazione (Argument): La prova soddisfa il requisito di "solidità", quindi è estremamente improbabile che si possa barare.
* Of Knowledge: La prova a conoscenza zero non può essere costruita senza accedere alle informazioni segrete (testimone). È difficile, se non impossibile, per un prover che non abbia il testimone, calcolare una prova a conoscenza zero valida.

La "chiave condivisa" menzionata in precedenza si riferisce ai parametri pubblici che il prover e il verificatore concordano di utilizzare per generare e verificare le prove. La generazione dei parametri pubblici (noti collettivamente come Common Reference String (CRS)) è un'operazione delicata a causa della sua importanza per la sicurezza del protocollo. Se l'entropia (casualità) utilizzata per generare la CRS finisce nelle mani di un prover disonesto, questi può calcolare prove false.

* zk-STARK

STARK è l'acronimo di "scalable transparent argument of knowledge". Le prove basate su STARK richiedono un'interazione minima tra il prover e il verificatore, il che le rende molto più veloci delle SNARK.

Gli ZK-STARK sono simili agli ZK-SNARK, con la differenza che sono:

* Scalabili: ZK-STARK è più veloce di ZK-SNARK nel generare e verificare prove quando la dimensione del testimone è maggiore. Con le prove STARK, i tempi del prover e della verifica aumentano solo leggermente al crescere del testimone (i tempi del prover e del verificatore dello SNARK aumentano linearmente con le dimensioni del testimone).
* Trasparenti: ZK-STARK si basa su una casualità verificabile pubblicamente per generare parametri pubblici per le prove e le verifiche, invece di un setup affidabile. Pertanto, sono più trasparenti rispetto agli ZK-SNARK.

Gli ZK-STARK producono prove più ampie rispetto agli ZK-SNARK, il che significa che in genere hanno un overhead di verifica più elevato. Tuttavia, ci sono casi (come la dimostrazione di grandi insiemi di dati) in cui gli ZK-STARK possono essere più convenienti degli ZK-SNARK.

* PLONK

Acronimo di "permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge", le PLONK utilizzano una configurazione di fiducia universale che può essere utilizzata con qualsiasi programma e può includere un gran numero di partecipanti.

* Bulletproofs

Le prove di validità sono brevi prove non interattive a conoscenza zero che non richiedono una configurazione fidata. Sono progettate per consentire transazioni private per le criptovalute.

Diverse varianti della conoscenza zero possono essere definite formalizzando il concetto intuitivo di ciò che si intende quando l'output del simulatore "assomiglia" all'esecuzione del protocollo di prova reale nei modi seguenti:

* Si parla di perfetta conoscenza zero se le distribuzioni prodotte dal simulatore e dal protocollo di prova sono distribuite esattamente allo stesso modo. Questo è ad esempio il caso del primo esempio sopra riportato.
* La conoscenza zero statistica significa che le distribuzioni non sono necessariamente identiche, ma sono statisticamente vicine, cioè la loro differenza statistica è una funzione trascurabile.
* Si parla di conoscenza zero computazionale se nessun algoritmo efficiente è in grado di distinguere le due distribuzioni.

Elenchiamo anche alcuni svantaggi dell'utilizzo di prove a conoscenza zero.

* Costi hardware

La generazione di prove a conoscenza zero comporta calcoli molto complessi, che è meglio eseguire su macchine specializzate. Poiché queste macchine sono costose, sono spesso fuori dalla portata di persone normali. Inoltre, le applicazioni che vogliono utilizzare la tecnologia zero-knowledge devono considerare i costi dell'hardware, che possono aumentare i costi per gli utenti finali.

* Costi di verifica delle prove

La verifica delle prove richiede anche calcoli complessi e aumenta i costi di implementazione della tecnologia a conoscenza zero nelle applicazioni. Questo costo è particolarmente rilevante nel contesto delle prove di calcolo. Ad esempio, gli ZK-rollup pagano ~ 500.000 gas per verificare una singola prova ZK-SNARK su Ethereum, mentre gli ZK-STARK richiedono tariffe ancora più elevate.

* Ipotesi di fiducia (trust assumptions)

In ZK-SNARK, la stringa di riferimento comune (parametri pubblici) viene generata una volta e può essere riutilizzata dalle parti che desiderano partecipare al protocollo a conoscenza zero. I parametri pubblici vengono creati attraverso una cerimonia di configurazione di fiducia, in cui si presume che i partecipanti siano onesti.

Ma non c'è modo per gli utenti di valutare l'onestà dei partecipanti e gli utenti devono prendere in parola gli sviluppatori. Gli ZK-STARK sono liberi da presupposti di fiducia, poiché la casualità utilizzata per generare la stringa è verificabile pubblicamente. Nel frattempo, i ricercatori stanno lavorando a configurazioni non fidate per gli ZK-SNARK per aumentare la sicurezza dei meccanismi di dimostrazione.

* Minacce del calcolo quantistico

Lo ZK-SNARK utilizza la crittografia a curva ellittica (ECDSA) per la crittografia. Sebbene l'algoritmo ECDSA sia per ora sicuro, lo sviluppo di computer quantistici potrebbe in futuro infrangere il suo modello di sicurezza.

ZK-STARK è considerato immune alla minaccia dell'informatica quantistica, in quanto utilizza hash resistenti alle collisioni per la crittografia. A differenza delle coppie di chiavi pubblico-privato utilizzate nella crittografia a curva ellittica, gli hash resistenti alle collisioni sono più difficili da violare per gli algoritmi di calcolo quantistico.

A livello matematico, possiamo citare:

1. Prova di conoscenza: In questo tipo di prova a conoscenza zero, una parte dimostra di conoscere un segreto senza rivelare il segreto stesso. Ciò avviene spesso utilizzando funzioni matematiche, come quelle che nascondono la conoscenza in un esponente.

* Esistono diversi modi per implementare le prove di conoscenza, ma una tecnica comune è quella di utilizzare funzioni matematiche che nascondono la conoscenza in un esponente. Ad esempio, supponiamo che il prover conosca un numero "x" che soddisfa una certa equazione, ma che non voglia rivelare "x" al verificatore. Il prover potrebbe invece rivelare il risultato dell'elevazione di un numero casuale 'r' a potenza di 'x' (cioè, r^x), senza rivelare 'x' stesso. Il verificatore può quindi controllare se l'equazione è soddisfatta calcolando la stessa funzione con i valori forniti dal prover.
* Se l'equazione è soddisfatta, il verificatore può essere certo che il prover conosce il valore di 'x', anche se non lo ha mai rivelato direttamente. Questa tecnica può essere utilizzata per dimostrare la conoscenza di una password, di una chiave privata o di qualsiasi altro valore segreto che soddisfi una relazione matematica.
* Un altro esempio di prova di conoscenza è il protocollo di identificazione di Schnorr, comunemente usato nelle firme digitali. In questo protocollo, il prover conosce una chiave privata "x" e la corrispondente chiave pubblica "y = g^x" (dove "g" è un generatore di un gruppo ciclico finito). Il prover vuole convincere il verificatore di conoscere la chiave privata 'x', senza rivelarla direttamente.

Il protocollo funziona come segue:

* Il verificatore invia un valore di sfida casuale "c" al prover.
* Il prover calcola un valore di risposta "r = x + c \* k", dove "k" è un altro valore casuale.
* Il prover invia 'r' al verificatore.
* Il verificatore controlla se 'g^r = y \* c^k'. Se questa equazione è valida, il verificatore può essere certo che il prover conosce la chiave privata 'x'.
* Se un aggressore cerca di impersonare il prover indovinando la chiave privata 'x', non sarà in grado di calcolare il valore di risposta corretto 'r' a meno che non conosca anche il valore casuale 'k'. La sicurezza del protocollo si basa sulla difficoltà di calcolare i logaritmi discreti nel gruppo ciclico generato da 'g'.

2. Crittografia a coppie: Questo tipo di crittografia utilizza accoppiamenti matematici per consentire una comunicazione sicura tra le parti senza rivelare i dati sottostanti. In sostanza, dati due input, permette di calcolare una funzione su tali input senza conoscere gli input stessi.

3. Prova indistinguibile del testimone: In questo tipo di prova, un verificatore non può determinare quale testimone sia stato utilizzato per produrre la prova. È utile in situazioni in cui si possono usare più testimoni per dimostrare un'affermazione, ma il prover vuole mantenere segreto il testimone effettivamente usato.

4. Calcolo a più parti: Si tratta di più parti che lavorano insieme per calcolare un risultato senza rivelare i propri input individuali. Ciascuna parte mantiene il proprio segreto, ma insieme sono in grado di produrre un risultato.

5. Firma ad anello: È un tipo di firma digitale che consente a un utente di firmare un messaggio senza rivelare la propria identità. La firma viene prodotta utilizzando un gruppo di possibili firmatari, noto come "anello", e gli estranei non possono determinare quale membro specifico dell'anello sia responsabile della firma.

## Consorzi internazionali coinvolti e finanziamenti europei

Uno dei principali consorzi internazionali è la Zcash Foundation, che è stata fondata nel 2017 per promuovere lo sviluppo e l'adozione di Zcash, una criptovaluta che utilizza la tecnologia ZKP per garantire la privacy degli utenti. La Zcash Foundation promuove la ricerca e lo sviluppo di nuove applicazioni per la tecnologia ZKP e collabora con diverse organizzazioni come la Electronic Frontier Foundation (EFF) e l'Open Privacy Research Society per promuovere la privacy online.

* In Europa, ci sono anche diversi finanziamenti disponibili per la ricerca e lo sviluppo della tecnologia ZKP. Ad esempio, Horizon 2020 è un programma di finanziamento dell'Unione europea per la ricerca e l'innovazione che ha finanziato diversi progetti legati alla tecnologia ZKP. Uno di questi progetti è stato "PRIViLEDGE", un progetto di ricerca che ha sviluppato un framework di sicurezza basato sulla tecnologia ZKP per garantire la privacy delle transazioni su blockchain.
* Il framework PRIViLEDGE è stato progettato per fornire una serie di strumenti di miglioramento della privacy per i sistemi blockchain. Questi strumenti si basano su diversi tipi di ZKP, come zk-SNARK e bulletproof, che consentono agli utenti di dimostrare la validità delle transazioni senza rivelare alcuna informazione sensibile.
  + Alcune delle caratteristiche principali del framework PRIViLEDGE sono:
    - Contratti intelligenti che preservano la privacy: Il framework consente la creazione di contratti intelligenti che possono essere eseguiti sulla blockchain preservando la privacy delle parti coinvolte.
    - Transazioni private: PRIViLEDGE consente transazioni private sulla blockchain, in cui l'importo della transazione e le parti coinvolte sono mantenute riservate.
    - Gestione dell'identità a tutela della privacy: Il framework consente la creazione di identità anonime che possono essere utilizzate per interagire con la blockchain senza rivelare alcuna informazione personale.
    - Condivisione sicura dei dati: Il framework fornisce un modo sicuro per gli utenti di condividere i dati sulla blockchain senza rivelare alcuna informazione sensibile.
    - Scalabilità: PRIViLEDGE è progettato per essere efficiente e scalabile, con bassi costi di transazione e tempi di elaborazione rapidi.

## Architettura e soluzioni

Un esempio comune di architettura usata con questo paradigma è la fiducia zero (ZT), che presuppone che tutti gli utenti, i dispositivi e le reti siano inaffidabili. Pertanto, lo ZT suggerisce una politica di sicurezza dinamica in cui utenti, dispositivi e reti sono sempre esaminati e monitorati.

Rispetto al paradigma di cybersecurity convenzionale, che presuppone che tutto ciò che si trova su un server aziendale sia affidabile, lo ZT è un paradigma di cybersecurity aggiornato che risponde meglio alle esigenze di sicurezza dell'ambiente di lavoro odierno. Oggi, infatti, i dipendenti utilizzano i propri dispositivi, il Wi-Fi pubblico e le piattaforme di cloud computing su cui le aziende hanno poco o nessun controllo e visibilità.

La ZT si basa su cinque principi fondamentali:

* Monitoraggio e convalida di utenti e dispositivi: Gli aggressori possono trovarsi sia all'interno che all'esterno della rete. Pertanto, il paradigma ZT prevede che l'identità e i privilegi degli utenti, nonché l'identità e la sicurezza dei dispositivi, vengano convalidati in modo sistematico. Di conseguenza, i login e le connessioni devono scadere regolarmente per costringere gli utenti e i dispositivi a una nuova verifica.
* Applicare il principio del minimo accesso: significa concedere agli utenti solo il livello di accesso di cui hanno bisogno. In questo modo si riduce l'esposizione di ciascun utente alle aree sensibili della rete e il potenziale di danno per gli hacker.
* Controllare l'accesso ai dispositivi: Le aziende devono sapere quanti dispositivi diversi tentano di accedere alla rete per garantire che ogni dispositivo sia autorizzato. Le organizzazioni devono esaminare tutti i dispositivi per assicurarsi che non siano stati violati. Questo principio riduce ulteriormente il vettore di attacco.
* Utilizzare la microsegmentazione: La microsegmentazione è il metodo di suddividere i perimetri di sicurezza in piccole regioni, in modo che le diverse aree della rete possano avere un accesso indipendente. Di conseguenza, la superficie di attacco si riduce.
* Prevenzione dei movimenti laterali: In un attacco informatico riuscito, i virus si diffondono rapidamente grazie agli spostamenti laterali. In questi casi, la localizzazione del paziente zero potrebbe non essere sufficiente a garantire la sicurezza della rete. È più facile prevenire la rapida diffusione dei virus se si impedisce la mobilità laterale. Pertanto, la messa in quarantena del dispositivo o dell'account utente del paziente zero può essere un metodo efficace per proteggere il resto della rete e degli utenti.

ZKA è un principio di progettazione. In parole povere, tutto ciò che si fa su un sistema Zero Knowledge viene crittografato prima di essere inviato al server e la chiave della crittografia non viene mai rivelata al fornitore.

* Il primo principio importante di ZKA è la crittografia end-to-end dei client che eseguono calcoli crittografici. Il server non sa nulla della natura dei dati. A proposito, a volte la ZKA viene definita "architettura senza conoscenza".
* In secondo luogo, tutte le operazioni sono effettuate su dati crittografati. Ciò significa che se si vuole aggiungere un nuovo record a un database, lo si deve aggiungere in forma criptata. Se si vuole condividere un dato, lo si deve fare in forma criptata. Si può anche eseguire una ricerca all'interno dei dati crittografati.

Questi principi non aggiungono ulteriore sicurezza nel senso comune del termine, ma garantiscono piuttosto che la crittografia lato client sia utilizzata correttamente. Gli algoritmi e i protocolli a conoscenza zero garantiscono che nessuna chiave, password, file o altro materiale sensibile venga mai trasferito in forma non cifrata o reversibile. In nessun momento le chiavi di crittografia o i file non crittografati sono visibili ai server o agli amministratori del servizio.

La ZTA è l'adozione di tecnologie e tecniche progettate per consentire l'implementazione di una mentalità di fiducia zero all'interno delle organizzazioni. Di conseguenza, la ZTA non è un'unica soluzione tecnologica, ma piuttosto un insieme di tecnologie che variano a seconda del settore e dell'azienda. In una ZTA vengono comunemente utilizzate le seguenti tecnologie:

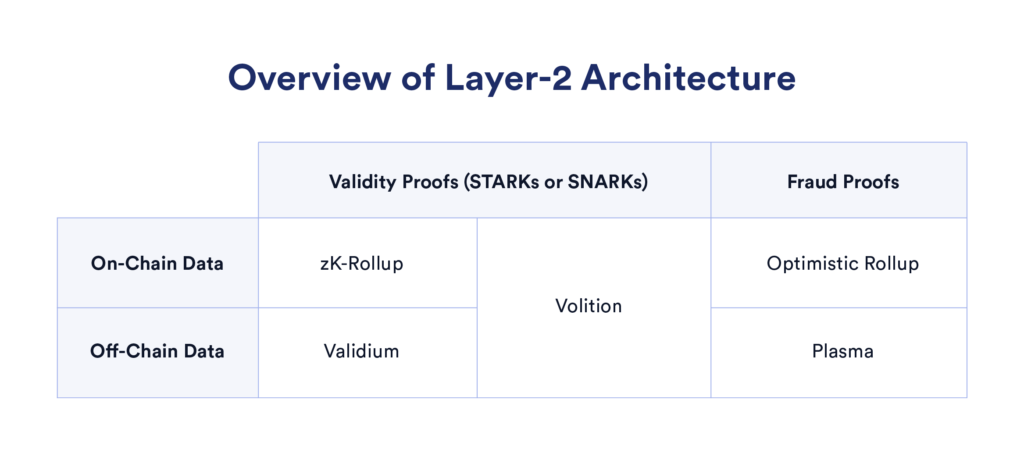
* Accesso alla rete a fiducia zero (ZTNA): È uno strumento che garantisce una convalida costante e una microsegmentazione per proteggere la rete dagli attacchi informatici.
  + ZTNA utilizza la microsegmentazione per fornire accesso solo alle risorse specifiche che un utente o un dispositivo richiede. In altre parole, anziché concedere l'accesso alla rete o alla sottorete completa, solo le risorse specifiche a cui l'utente o il dispositivo ha bisogno di accedere sono rese disponibili. ZTNA fornisce anche una convalida costante dell'identità dell'utente e del dispositivo, garantendo che solo quelli autorizzati possano accedere alle risorse.
* Perimetro definito dal software (SDP): È la tecnologia che consente la microsegmentazione e l'implementazione del principio del minimo accesso. L'SDP presenta un netto vantaggio rispetto a una VPN, poiché la connessione a una VPN consente all'utente di accedere all'intera rete.
  + SDP utilizza la microsegmentazione per creare un perimetro virtuale intorno alle risorse di rete, in modo che solo gli utenti o i dispositivi autorizzati possano accedere alle risorse specifiche. Questo approccio è molto diverso da quello tradizionale basato su VPN, in cui l'accesso è concesso all'intera rete. Inoltre, SDP fornisce un'implementazione del principio del minimo accesso, ovvero l'accesso solo alle risorse necessarie per svolgere il lavoro richiesto.
* Secure access service edge (SASE): È la soluzione unificata di rete e sicurezza basata sull'approccio ZT. SASE combina la sicurezza degli accessi alla rete (ZTNA) con altre funzionalità di sicurezza, come i firewall gestiti nel cloud, la sicurezza web e la protezione dal malware, il tutto offerto come servizio. Questo approccio consente di proteggere i dati e le risorse di una rete distribuita, garantendo la sicurezza degli accessi ovunque gli utenti si trovino. Inoltre, SASE fornisce una gestione centralizzata delle politiche di sicurezza, semplificando la gestione della sicurezza della rete.

Possiamo determinare subito alcuni benefici nell’implementazione di un’architettura ZTA:

* Riduzione della superficie di attacco: Un attacco informatico riuscito può colpire solo una parte della rete aziendale grazie al principio del minimo accesso e alla microsegmentazione con SDP. Di conseguenza, la ZTA riduce il costo dei software malware come i ransomware. È fondamentale per le aziende, dato che gli attacchi ransomware sono aumentati del 105% nel 2021 rispetto al 2020.
* Fornisce una maggiore visibilità: Le aziende possono conoscere l'ora, la posizione e le applicazioni coinvolte in ogni richiesta di accesso una volta impostato il monitoraggio per coprire tutte le risorse e le attività. In questo modo ci vuole meno tempo per trovare il paziente zero e ricostruire la cybersecurity.
* Protezione contro le minacce interne: Le violazioni e gli abusi dei dati possono essere causati da dipendenti disonesti o da errori dei dipendenti. Le aziende sono protette da questi pericoli in due modi quando vengono implementati i principi della ZT:
  + Il monitoraggio regolare della salute dei dispositivi riduce il rischio di ingresso di codice malware nella rete.
  + Il concetto di accesso minimo garantisce che il personale disonesto non abbia accesso a tutti i dati aziendali. La ZTA facilita inoltre l'individuazione dei dipendenti disonesti, perché aumenta la visibilità.
* Semplificare l'accesso degli utenti: L'accesso predeterminato degli utenti elimina la necessità di un'approvazione amministrativa continua. I dipendenti dispongono già di tutti gli strumenti e i dati di cui hanno bisogno. In questo modo, aumenta l'efficienza operativa.
* Consente di lavorare in modo moderno e sicuro: ZTA offre un ambiente di lavoro sicuro ai dipendenti mobili, proprio come se lavorassero negli uffici aziendali utilizzando i dispositivi aziendali. Questo aumenta la flessibilità organizzativa e l'accessibilità dell'azienda a un maggior numero di talenti.

* Migliorare la conformità normativa: Le organizzazioni sono preoccupate per i nuovi standard di conformità normativa, come il Regolamento generale sulla protezione dei dati (GDPR), il California Consumer Privacy Act (CCPA), l'Health Insurance Portability and Accountability Act (HIPAA) e altri. Il problema di questi requisiti è determinare come salvaguardare e proteggere i dati. Ogni volta che viene effettuato un movimento in un'architettura Zero Trust, l'identità e il payload vengono convalidati, il che aiuta a bloccare l'attacco prima che i dati vengano raggiunti.

A livello di soluzioni basate su ZKP, possiamo dettagliare la seguente immagine:



Riferimento: <https://blog.chain.link/zero-knowledge-proof-projects/>

* + Zero Knowledge Rollup (zk-Rollup), sfruttare la funzionalità principale dei rollup attraverso l'integrazione delle sidechain. In generale, le sidechain consentono a una parte di dimostrare a un'altra che una transazione è valida senza rivelare alcuna informazione oltre alla validità della transazione stessa.
  + Più specificamente, i protocolli zk-Rollup facilitano le interazioni tra transactor e relayer:
    - I transactor creano e trasmettono alla rete i dati delle loro transazioni. Queste informazioni comprendono un indirizzo "da" e "a" indicizzato, il valore della transazione, la commissione di rete e un numero utilizzato una sola volta (nonce). Gli indirizzi indicizzati riducono le risorse di elaborazione, mentre il valore della transazione genera un importo di deposito e di prelievo. I contratti intelligenti registrano quindi gli indirizzi in un Merkle Tree e il valore della transazione in un altro.
    - I relayer sono responsabili della raccolta delle transazioni e della creazione di rollup. I relayer generano una prova Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) che confronta lo stato della blockchain prima e dopo ogni transazione (cioè i saldi dei portafogli). Le modifiche risultanti raggiungono la mainchain in un hash verificabile. Anche se praticamente chiunque può agire come relayer, deve prima puntare la propria criptovaluta in uno smart contract, che lo incentiva ad agire in buona fede.
    - Uno Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) è un tipo di prova crittografica utilizzata per garantire la privacy nei sistemi di registro distribuito basati su blockchain. Funziona dimostrando che una parte è in possesso di dati specifici senza rivelare effettivamente i dati alla rete, utilizzando una chiave segreta prima che la transazione venga trasmessa. zk-SNARKS è diventato importante con Zcash, Monero e altri protocolli blockchain basati sulla privacy.
  + Utilizzando zk-Rollups, è possibile supportare un'ampia varietà di funzionalità per token fungibili, token non fungibili (NFT) e applicazioni decentralizzate (dApp).
    - Loopring, protocollo di scambio decentralizzato (DEX) che consente agli utenti di scambiare token digitali in modo rapido e sicuro senza la necessità di intermediari centralizzati. Loopring utilizza un modello di scambio a anelli che consente agli utenti di scambiare più token contemporaneamente in modo efficiente e sicuro. Inoltre, Loopring è progettato per essere altamente scalabile, consentendo a un gran numero di utenti di scambiare token contemporaneamente senza avere problemi di congestione della rete.
    - dYdX, protocollo di trading decentralizzato che consente agli utenti di effettuare scambi di criptovalute a margine e di effettuare prestiti in modo sicuro e trasparente. dYdX consente agli utenti di scambiare criptovalute con una leva finanziaria, il che significa che gli utenti possono effettuare scambi con un importo che supera il loro saldo disponibile. Inoltre, dYdX consente agli utenti di effettuare prestiti di criptovalute con tassi di interesse variabili, consentendo loro di guadagnare interessi sui loro depositi di criptovalute.
    - Hermez
      * La piattaforma Hermez utilizza zk-Rollups per ottimizzare trasferimenti di token sicuri e a basso costo sulla blockchain di Ethereum. Durante il processo di trasferimento, i fondi sono conservati in uno smart contract sulla mainchain mentre le prove crittografiche zk-SNARK hanno origine fuori dalla catena.
      * Questi zk-SNARK aiutano a verificare ogni lotto di transazioni registrate sulla mainchain, alleviando la congestione della rete e consentendo velocità di elaborazione costanti. Inoltre, poiché tutte le transazioni vengono registrate sulla mainchain, chiunque può ricostruire lo stato attuale e la storia delle transazioni. Questa dinamica aiuta a mitigare la censura e la centralizzazione dei coordinamenti zk-Rollup che raggruppano le transazioni. Nel 2021, Hermez è stata acquisita dal popolare progetto di scalatura Ethereum Layer-2 Polygon (MATIC).
    - zkSync
      * Proveniente dal team di Matter Labs, zkSync funziona come una soluzione di scalatura Ethereum Layer-2 che riduce le commissioni di gas derivanti dalle transazioni sulla rete. Attraverso l'infrastruttura zk-Rollup, i token ether (ETH) e ERC-20 sono detenuti da uno smart contract sulla mainchain, mentre lo storage computazionale avviene fuori dalla catena. Come altri protocolli di trasferimento di valore, gli zk-SNARKS sono generati e verificati dal contratto della mainchain. Come per i protocolli alternativi, questi zk-SNARK convalidano ogni transazione in uno specifico blocco rollup e i dati risultanti sono pubblicamente disponibili.
    - Aztec
      * Il protocollo Aztec utilizza due programmi di "circuito" zk-SNARK codificati: un circuito di privacy e un circuito di rollup. Il circuito di privacy assicura l'accuratezza di una singola transazione e invia le transazioni direttamente dall'hardware dell'utente per preservare la privacy. Il circuito di rollup è responsabile della convalida dell'accuratezza di ogni lotto di prove, attualmente impostato su 128 prove.
      * Il circuito di rollup gestisce anche un database di dati crittografati delle transazioni. Sebbene tutte le prove di zk-Rollup in uso siano generate da Aztec, l'azienda prevede di decentralizzare questo servizio affidando il calcolo a terzi. Indipendentemente dal fornitore del servizio, i clienti vedranno solo i risultati crittografati delle prove di privacy, eliminando gli attacchi di censura poiché tutte le transazioni appariranno come numeri casuali.
  + Limitazioni:
    - (i) Poiché i dati delle transazioni eseguite vengono raggruppati e pubblicati sulla catena principale, la scalabilità è limitata. La scalabilità con i rollup può arrivare a 100 volte, ma non può scalare la Blockchain all'infinito.
    - (ii) Sebbene la congestione della rete della catena principale sia alleviata poiché tutto il lavoro di calcolo viene svolto fuori dalla catena sul livello 2 dei rollup, le transazioni vengono eseguite eseguendo una versione dell'EVM nei rollup. Pertanto, anche sui rollup viene eseguita la stessa esecuzione della catena principale di Ethereum e agli utenti vengono addebitate le tariffe del gas. Ma le tariffe del gas sul livello rollup sono molto più economiche che su Ethereum.
  + Validium
  + I Validium, un tipo di ZK Rollup in cui invece di memorizzare una parte dei dati sulla catena, tutti i dati vengono memorizzati fuori dalla catena. Combinano le prove di validità con l'archiviazione dei dati fuori dalla catena per migliorare la scalabilità. Le prove di validità sono ancora pubblicate sulla catena di base, mentre i dati sono archiviati fuori dalla catena. Questo migliora significativamente il throughput e riduce i costi del gas.
  + Sebbene si tratti di un'architettura molto più efficiente e scalabile rispetto agli zk-rollup, presenta il rischio che attori malintenzionati rendano i dati non disponibili e che gli utenti non possano prelevare i loro fondi. Il problema della disponibilità dei dati viene superato con sistemi di tipo proof-of-stake che utilizzano incentivi criptoeconomici per garantire che i dati siano archiviati da molti nodi diversi e sempre disponibili. È importante notare che, sebbene questi attori malintenzionati possano bloccare le transazioni, non possono rubare direttamente i fondi degli utenti.
* Alcuni progetti basati su Validium:
  + - Immutable X
      * Il team di Immutable X ha costruito il suo protocollo per ottimizzare il conio e la negoziazione di NFT basati su Ethereum. Il protocollo mira a fornire agli utenti conferme istantanee delle transazioni, una migliore scalabilità e l'assenza di spese per il gas, il tutto rimanendo non custodiale. Attraverso l'uso di zk-Rollup, Immutable X sposta migliaia di transazioni dalla mainchain e pubblica la prova risultante sulla mainchain, dove uno smart contract verifica le transazioni. Come molti altri protocolli, i beni degli utenti sono trattenuti in uno smart contract della mainchain fino alla pubblicazione di una prova valida.
    - Mercato di lancio DeversiFi (DLM)
      * Oltre a fornire un protocollo di scambio decentralizzato (DEX), DeversiFi ha anche introdotto i DeversiFi Launch Markets (DLM). Questi mercati integrano elementi di asta inversa e liquidità continua per stabilire i prezzi di mercato dei token attraverso la partecipazione. Poiché i DLM hanno origine sul Layer 2, non ci sono commissioni di gas e i partecipanti mantengono il controllo completo dei loro fondi.
  + Sorare, piattaforma di fantasy football basata sulla blockchain Ethereum che consente agli utenti di collezionare, negoziare e competere con carte collezionabili digitali (NFT) di giocatori di calcio.
    - Essa consente agli utenti di acquistare carte collezionabili digitali di giocatori di calcio di tutto il mondo, con ogni carta che rappresenta un giocatore specifico. Ogni carta NFT è unica e può essere posseduta solo da un singolo utente, il che significa che gli utenti possono collezionare e scambiare le carte tra di loro in modo simile alle carte collezionabili fisiche.
    - Una volta che gli utenti hanno acquistato le carte, possono utilizzarle per formare una squadra di fantasy football. Gli utenti possono quindi competere contro altri utenti per vincere premi in criptovaluta, in base alle prestazioni dei giocatori nella vita reale.
    - Sorare utilizza la tecnologia blockchain per garantire la proprietà e l'autenticità delle carte collezionabili digitali. Ogni carta NFT è registrata sulla blockchain Ethereum, il che significa che gli utenti possono verificare la proprietà e l'autenticità delle loro carte in modo sicuro e trasparente.
    - Inoltre, Sorare utilizza la tecnologia di prova a conoscenza zero per garantire la privacy degli utenti. Ciò significa che gli utenti possono partecipare alle competizioni senza dover rivelare le proprie strategie di formazione della squadra o le carte che possiedono.

Il concetto è importante: si parla infatti anche di validity proofs, altro nome delle ZKP, metodo di verifica delle transazioni che si svolge tra un prover, che sta creando una prova per alcune informazioni, e un verificatore, che verifica la prova senza condividere alcuna informazione tra i due.

* L'informazione condivisa tra un prover e un verificatore è chiamata testimone ed è tipicamente la soluzione di una complessa equazione matematica. In sostanza, il prover deve dimostrare di conoscere accuratamente il testimone e il verificatore deve essere in grado di accertare in modo affidabile se il prover conosce il testimone.
* Le prove di validità sono progettate per essere difficili da infrangere e si basano su una tecnica crittografica nota come impegni polinomiali. Negli impegni polinomiali, le informazioni di ogni fase del calcolo di verifica sono codificate in polinomi e un'espressione polinomiale fattorizzata può sostituire un gran numero di equazioni tra numeri.

Verificando le equazioni polinomiali, si verificano implicitamente i calcoli numerici, ma il processo di hashing di questi polinomi è complicato. I tre principali schemi di hashing dei polinomi utilizzati per gli impegni polinomiali sono:

* KZG (Kate) Polynomial Commitments, tipo di crittografia a chiave pubblica utilizzata per verificare l'integrità dei dati. In particolare, KZG Polynomial Commitments vengono utilizzati per creare un impegno su un polinomio, che può essere verificato senza rivelare il polinomio stesso.
  + Un esempio di come KZG Polynomial Commitments possono essere utilizzati nella crittografia è la creazione di una firma digitale. In questo caso, un utente crea un polinomio che rappresenta la chiave di firma, quindi crea un impegno su questo polinomio utilizzando la tecnologia KZG. Quando viene richiesta la verifica della firma, l'utente può dimostrare che il polinomio utilizzato per creare l'impegno corrisponde alla chiave di firma senza rivelare il polinomio stesso.
* Bulletproofs, che consentono di verificare la correttezza di una transazione senza dover rivelare gli importi specifici delle transazioni o le chiavi pubbliche coinvolte. Ciò consente di mantenere la privacy degli utenti, mentre si garantisce la correttezza delle transazioni.
  + Un esempio di utilizzo è la verifica delle transazioni in una blockchain. Invece di rivelare gli importi specifici delle transazioni o le chiavi pubbliche coinvolte, Bulletproofs consentono di dimostrare che la transazione è stata effettuata correttamente senza rivelare queste informazioni.
  + Bulletproofs utilizzano un sistema di prova a conoscenza zero (zk-SNARK) per dimostrare la correttezza della transazione senza rivelare informazioni specifiche sulla transazione stessa. Ciò significa che gli utenti possono verificare la correttezza delle transazioni senza dover rivelare le loro identità o le informazioni specifiche sulla transazione.
  + È importante notare che Bulletproofs non sono completamente privati. Sebbene non rivelino le informazioni specifiche della transazione, possono fornire informazioni sulle dimensioni delle transazioni, che potrebbero essere utilizzate per dedurre informazioni sulla transazione stessa. Tuttavia, se utilizzati correttamente, Bulletproofs possono fornire un livello aggiuntivo di sicurezza e privacy per le transazioni crittografiche.
* FRI (Fast Reed-Solomon Interactive Oracle Proofs of Proximity), che consente di dimostrare che un valore si trova in prossimità di un insieme di valori noti, senza dover rivelare il valore specifico.
  + Un esempio di come FRI può essere utilizzato nella crittografia è la verifica dell'accesso a una risorsa senza rivelare l'identità dell'utente che richiede l'accesso. Invece di rivelare l'identità dell'utente, FRI consente di dimostrare che l'utente ha accesso alla risorsa senza rivelare l'identità dell'utente stesso.
  + FRI utilizza un sistema di prova a conoscenza zero (zk-SNARKs) per dimostrare la prossimità di un valore a un insieme di valori noti. Ciò significa che gli utenti possono dimostrare l'accesso a una risorsa senza rivelare le loro identità o i valori specifici coinvolti.

Similmente alle precedenti, parliamo delle prove di frode (fraud proofs), note anche come prove di errore, prove presentate da un verificatore che contesta lo stato di una transazione. In base all'implementazione, la prova di frode esamina un segmento delle transazioni e tenta di convalidarle.

Ecco una spiegazione semplice:

* Se la prova di frode individua un errore, le transazioni inserite nel batch vengono rimosse e il batch viene riportato a uno stato precedente, verificabile e corretto.
* Se non vengono presentate prove di frode durante il periodo di contestazione, si presume ottimisticamente che il cambiamento di stato sia corretto.

Le prove di frode funzionano confrontando le radici di Merkle e verificando le radici dello stato iniziale e finale attraverso un singolo ciclo di calcolo (come Optimism) o un calcolo a più cicli (come Arbitrum).

* La blockchain funziona su una struttura di dati nota come Albero di Merkle, che contiene ogni transazione come una foglia dell'albero e i rami successivi rappresentati da hash sempre più complessi dell'albero.
* Il nodo radice, noto anche come Merkle Root, è un hash che condensa efficacemente i dati in modo che gli utenti non debbano scaricare costantemente l'intera catena principale.
* Se un verificatore vuole contestare un cambiamento di stato di una transazione, deve solo presentare la radice post-statale corrente e parti specifiche dell'albero di Merkle che possono essere utilizzate per calcolare la radice post-statale corretta. Se i due non sono d'accordo, le modifiche allo stato della transazione vengono annullate e l'hash viene ripristinato su una radice di stato provatamente corretta.

Le prove ZK e le prove di frode presentano numerose differenze, tra cui la quantità di calcoli necessari, il tempo necessario per convalidare una transazione, la sicurezza e la difficoltà di implementazione.

1. Le prove di validità sono più impegnative dal punto di vista computazionale delle prove di frode

Le prove ZK sono intrinsecamente difficili da convalidare dal punto di vista matematico e di solito richiedono un'intensa attività di calcolo, data la natura tecnica richiesta da un processo di verifica a conoscenza zero.

Le prove di frode sono tipicamente più economiche per lotto, con circa 40.000 gas, mentre le prove ZK SNARK richiedono 500.000 gas. Tuttavia, le ZK SNARK sono più economiche sulla catena perché i rollup ottimistici devono pubblicare tutti i dati sulla blockchain principale per una prova di frode che legittimi o confuti un risultato.

1. Le prove di validità sono istantanee, mentre le prove di frode hanno un ritardo di contestazione.

Una differenza importante tra le prove ZK e le prove di frode è che mentre le prove ZK convalidano una transazione immediatamente, le prove di frode hanno un ritardo intrinseco nel tempo di contestazione (DTD) che rallenta le transazioni. Solo se i verificatori non hanno presentato prove di frode per un determinato lotto, questo sarà effettivamente pubblicato su Ethereum.

1. Le prove di validità sono più decentralizzate e sicure dei dati

Poiché le prove ZK richiedono un'interazione minima (ad esempio, solo la condivisione di una prova a un verificatore) e questo processo può essere fatto in modo sicuro, sono molto decentralizzate.

Inoltre, poiché le prove sono a conoscenza zero e perfettamente accurate, le prove di validità proteggono la privacy degli utenti e riducono al minimo il rischio di gravi minacce come gli attacchi al 51% della catena L1.

I rollup ottimistici, invece, richiedono che il verificatore invii una prova di frode, che può essere intercettata o sottoposta a DDoS per impedire che una sfida sullo stato della transazione venga trasmessa al batch.

1. Le prove di validità sono più difficili da implementare

Mentre i rollup ottimistici, e di conseguenza le prove di frode, possono funzionare su qualsiasi EVM o macchina virtuale ottimistica (OVM), le prove a conoscenza zero e i rollup ZK richiedono macchine virtuali specializzate chiamate macchine virtuali Ethereum a conoscenza zero (zkEVM). Queste macchine virtuali sono in grado di eseguire contratti intelligenti in un modo che funziona con il calcolo ZK e le prove di validità crittografica.

Fino a poco tempo fa si pensava che le zkEVM fossero solo teoricamente possibili, e ancora oggi è difficile avvolgere le EVM per supportare le prove ZK. Tuttavia, ci sono nuovi sviluppi nello spazio ZK che consentono di aumentare il throughput e la scalabilità delle prove ZK.

In particolare, Polygon sta creando la propria tecnologia di rollup, che utilizza ZK SNARK ricorsivi per eseguire in modo più efficiente le transazioni fuori dalla catena prima di tornare alla catena principale. Le prove ricorsive funzionano provando più blocchi di transazioni alla volta e poi provando anche un blocco aggregato.

* Le volitions, che combinano sia gli zk-rollup che i validium e consentono agli utenti di scegliere (da qui il nome) tra entrambe le soluzioni di scaling, poiché condividono un'unica radice di stato. Anche se si verificasse un attacco malevolo sul lato validium della volizione, i fondi sul lato zk-rollup sarebbero comunque al sicuro.
  + Ciò consente alle entità disposte a pagare commissioni più elevate per le maggiori garanzie di sicurezza di uno zk-rollup di interagire in modo nativo con i partecipanti che preferiscono i minori costi di transazione di una volizione, come ad esempio in un DEX dove un market maker sta fornendo centinaia di milioni di liquidità mentre un trader al dettaglio può avere solo poche posizioni aperte.
  + Queste transizioni di stato vengono eseguite dagli utenti o dagli smart contract per aggiornare lo stato di uno specifico protocollo di livello 2, senza richiedere un corrispondente aggiornamento della blockchain sottostante.

Le transizioni sono un concetto importante per la scalabilità del layer-2, perché consentono un aumento significativo del throughput delle transazioni, senza richiedere un corrispondente aumento della capacità della blockchain sottostante. Questo risultato si ottiene spostando gran parte dell'elaborazione delle transazioni fuori dalla catena, nella soluzione di livello 2.

* + Un esempio di come le volizioni possono essere utilizzate nella pratica è rappresentato dai canali di pagamento. Un canale di pagamento è una soluzione di livello 2 che consente a due parti di effettuare transazioni tra loro più volte, senza che ogni transazione venga registrata sulla blockchain sottostante. Le parti possono invece eseguire transizioni di stato fuori dalla catena (volizioni) per aggiornare il saldo del canale di pagamento tra di loro. Una volta che le parti sono pronte a saldare il saldo finale, possono inviare una singola transazione alla blockchain che riflette il saldo finale, invece di richiedere transazioni multiple per ogni singolo pagamento.

Le prove di validità sono poi basate su SNARK e su STARK.

* SNARK è l'acronimo di "zero-knowledge succinct non-interactive argument on knowledge". Uno SNARK è un tipo di prova crittografica di dimensioni ridotte e facile da verificare. Gli SNARK generano una prova crittografica utilizzando le curve ellittiche, che presuppongono che sia impossibile trovare il logaritmo discreto di un elemento casuale della curva ellittica a partire da un punto base pubblicamente noto. Il calcolo delle curve ellittiche è meno dispendioso dal punto di vista computazionale rispetto al calcolo delle funzioni di hashing utilizzate dalle STARK, motivo per cui i protocolli basati sulle SNARK possono essere più efficienti dal punto di vista del gas.
* STARK è l'acronimo di "zero-knowledge scalable transparent argument of knowledge". È un tipo di prova crittografica che richiede un'interazione minima o nulla tra il prover e il verificatore. I vantaggi principali delle STARK rispetto alle SNARK sono che hanno tempi di prover rapidi e sono più facili da scalare in quanto offrono una maggiore potenza di calcolo. Inoltre, l'uso di funzioni di hash li rende resistenti alla quantistica.

Listiamo dei progetti basati su zk-STARK:

* StarkEx

StarkEx è una soluzione di scalabilità di livello 2 costruita su Ethereum che utilizza le prove STARK per convalidare le transazioni auto-custodite, consentendo di costruire applicazioni di trading e di pagamento su di essa. Tuttavia, StarkEx non supporta la funzionalità di smart contract che consente di creare dApp complete. StarkEx è progettato per essere altamente scalabile, consentendo agli utenti di scambiare un gran numero di token con un basso costo e alta velocità. Inoltre, StarkEx offre una maggiore privacy rispetto alle soluzioni di scambio centralizzate, poiché non richiede la condivisione delle chiavi private degli utenti.

* StarkNet

StarkNet è una piattaforma generica che consente agli sviluppatori di distribuire contratti intelligenti su uno zk-rollup basato su Ethereum. Entrambe le principali dApp di Ethereum, Aave e Maker, saranno lanciate su StarkNet. In particolare, gli zk-rollup StarkEx possono essere lanciati su StarkNet per aumentare la scalabilità di un'applicazione.

Per sfruttare appieno il calcolo avanzato e la scalabilità possibili con STARK, StarkWare ha creato un nuovo linguaggio di programmazione altamente efficiente e Turing-completo per la generazione di prove STARK, chiamato Cairo. StarkNet è progettato per essere compatibile con gli strumenti e le infrastrutture esistenti di Ethereum, consentendo ai dApp sviluppati con StarkNet di essere eseguiti sulla rete Ethereum con un'alta efficienza e sicurezza.

StarkWare offre una serie di modalità di Data Availability (DA) che i clienti possono scegliere in base alle loro priorità.

Esistono tre approcci alla Data Availability per le prove STARK, tutti già enunciati:

* Rollup: il libro mastro viene pubblicato direttamente sulla blockchain
* Validium: un comitato per la disponibilità dei dati protegge il libro mastro, con solo un hash memorizzato sulla catena.
* Volition: le app possono permettere agli utenti di scegliere la modalità DA - Rollup o Validium - per ogni singola transazione.

Gli utenti inviano transazioni sul Layer 2 (StarkEx o StarkNet), che vengono raggruppate e inviate a un prover STARK. Questo prover STARK conosce lo stato del libro mastro prima e dopo l'elaborazione delle transazioni. Il prover produce una prova STARK che attesta la validità del nuovo stato del libro mastro dopo l'esecuzione delle transazioni. Il nuovo stato e la prova STARK vengono inviati al verificatore STARK della catena. La verifica di questa prova avviene autonomamente tramite uno smart contract immutabile su Ethereum.

Questa architettura offre il meglio dei due mondi: possiamo avere bassi costi di transazione, pur avendo Ethereum nel mezzo come arbitro neutrale. Ethereum come arbitro non è solo un aspetto piacevole, ma fornisce una sicurezza fondamentale all'utente finale. Un utente che effettua transazioni può ora essere sicuro che i suoi fondi sono protetti da Ethereum e che le transazioni sono immutabili una volta verificate su Ethereum. Inoltre, l'utente può contare su una custodia completa dei propri fondi. L'autodeposito è importante perché assicura che l'utente abbia accesso ai propri fondi in ogni momento, senza affidarsi a terzi.

Invece, per quanto riguarda progetti basati su zk-SNARK:

* Zcash, precedentemente chiamato ZeroCash in riferimento alla prova a conoscenza zero utilizzata per supportare le sue transazioni che preservano la privacy, è una delle prime criptovalute e ha contribuito a rendere pionieristico l'uso della tecnologia a conoscenza zero nel settore.
  + Zcash utilizza la tecnologia di prova a conoscenza zero per garantire la privacy degli utenti. Ciò significa che le transazioni su Zcash possono essere verificate senza la necessità di rivelare le informazioni specifiche sulla transazione stessa, come ad esempio l'importo trasmesso o l'indirizzo del mittente e del destinatario. Questo rende Zcash una delle criptovalute più private e anonime disponibili.
  + Inoltre, Zcash offre due tipi di indirizzi: gli indirizzi trasparenti, simili agli indirizzi Bitcoin normali, e gli indirizzi privati, chiamati "z-address". Gli indirizzi privati consentono agli utenti di effettuare transazioni completamente anonime, poiché non è possibile tracciare le transazioni in modo pubblico sulla blockchain. Tuttavia, le transazioni verso gli indirizzi privati richiedono più risorse computazionali rispetto alle transazioni verso gli indirizzi trasparenti.
* Il protocollo ZigZag è un exchange decentralizzato che utilizza un order book per le coppie di trading ERC-20, a differenza della maggior parte dei DEX, che utilizzano progetti di market maker automatizzati. È la scalabilità di zk-rollup che rende fattibile il design del libro degli ordini. Qualsiasi token nel registro di zkSync può essere quotato su ZigZag. Il protocollo opera attualmente su zkSync 1.0, ma ha in programma il lancio su zkSync 2.0 e StarkNet.
  + ZigZag Protocol utilizza una serie di smart contract per automatizzare il processo di scambio di token tra diverse blockchain, garantendo che tutte le transazioni siano eseguite in modo sicuro e trasparente.
* Il protocollo Mina è un progetto di blockchain leggera a prova di conoscenza zero che utilizza gli SNARK per produrre blocchi di dimensioni limitate a 22kb. I progetti possono costruire applicazioni su Mina con funzionalità complete di smart contract.
  + Mina Protocol consente agli sviluppatori di creare applicazioni decentralizzate utilizzando una lingua di programmazione familiare come Javascript, rendendo la creazione di applicazioni decentralizzate accessibile a un pubblico più ampio.

## Casi d’uso reali

* Pagamenti anonimi

I pagamenti con carta di credito sono spesso visibili a più parti, tra cui il fornitore dei pagamenti, le banche e altre parti interessate (ad esempio, le autorità governative). Se da un lato la sorveglianza finanziaria ha dei vantaggi per l'identificazione di attività illegali, dall'altro mina la privacy dei cittadini comuni.

Le criptovalute sono state concepite per fornire agli utenti un mezzo per condurre transazioni private e peer-to-peer. Ma la maggior parte delle transazioni in criptovalute sono apertamente visibili sulle blockchain pubbliche. Le identità degli utenti sono spesso pseudonime e collegate intenzionalmente a identità del mondo reale (ad esempio includendo gli indirizzi ETH nei profili Twitter o GitHub) o possono essere associate a identità del mondo reale utilizzando un'analisi di base dei dati on e off-chain.

Esistono specifiche "monete della privacy" progettate per transazioni completamente anonime. Le blockchain incentrate sulla privacy, come Zcash e Monero, proteggono i dettagli delle transazioni, compresi gli indirizzi del mittente/destinatario, il tipo di asset, la quantità e la cronologia della transazione.

Inserendo la tecnologia zero-knowledge nel protocollo, le reti blockchain incentrate sulla privacy consentono ai nodi di convalidare le transazioni senza dover accedere ai dati delle transazioni.

Le prove a conoscenza zero vengono applicate anche per anonimizzare le transazioni sulle blockchain pubbliche. Un esempio è Tornado Cash, un servizio decentralizzato e non custodiale che consente agli utenti di condurre transazioni private su Ethereum. Tornado Cash utilizza prove di conoscenza zero per offuscare i dettagli delle transazioni e garantire la privacy finanziaria. Purtroppo, trattandosi di strumenti di privacy "opt-in", sono associati ad attività illecite. Per superare questo problema, la privacy deve diventare l'opzione predefinita sulle blockchain pubbliche.

* Protezione dell'identità

Gli attuali sistemi di gestione dell'identità mettono a rischio le informazioni personali. Le prove a conoscenza zero possono aiutare gli individui a convalidare l'identità proteggendo al contempo i dettagli sensibili.

Le prove a conoscenza zero sono particolarmente utili nel contesto dell'identità decentralizzata. L'identità decentralizzata (descritta anche come "identità auto-sovrana") dà all'individuo la possibilità di controllare l'accesso agli identificatori personali. Dimostrare la propria cittadinanza senza rivelare i dati del codice fiscale o del passaporto è un buon esempio di come la tecnologia zero-knowledge consenta l'identità decentralizzata.

* Autenticazione

Per utilizzare i servizi online è necessario dimostrare la propria identità e il diritto di accedere a tali piattaforme. Spesso è necessario fornire informazioni personali, come nomi, indirizzi e-mail, date di nascita e così via. Potrebbe anche essere necessario memorizzare lunghe password o rischiare di perdere l'accesso.

Le prove a conoscenza zero, tuttavia, possono semplificare l'autenticazione sia per le piattaforme che per gli utenti. Una volta generata una prova ZK utilizzando input pubblici (ad esempio, dati che attestano l'appartenenza dell'utente alla piattaforma) e privati (ad esempio, i dati dell'utente), l'utente può semplicemente presentarla per autenticare la propria identità quando deve accedere al servizio. Questo migliora l'esperienza degli utenti e libera le organizzazioni dalla necessità di memorizzare enormi quantità di informazioni sugli utenti.

* Calcolo verificabile

Il calcolo verificabile è un'altra applicazione della tecnologia a conoscenza zero per migliorare i progetti della blockchain. La computazione verificabile ci permette di esternalizzare il calcolo a un'altra entità mantenendo risultati verificabili. L'entità invia il risultato insieme a una prova che verifica che il programma sia stato eseguito correttamente.

Il calcolo verificabile è fondamentale per migliorare la velocità di elaborazione delle blockchain senza ridurre la sicurezza. Per comprendere questo aspetto è necessario conoscere le differenze tra le soluzioni proposte per scalare Ethereum.

Le soluzioni di scalabilità on-chain, come lo sharding, richiedono una modifica estesa del livello di base della blockchain. Tuttavia, questo approccio è molto complesso e gli errori di implementazione possono minare il modello di sicurezza di Ethereum.

Le soluzioni di scaling off-chain non richiedono la riprogettazione del protocollo principale di Ethereum. Si basano invece su un modello di calcolo esternalizzato per migliorare il throughput del livello base di Ethereum.

Ecco come funziona in pratica:

* Invece di elaborare ogni transazione, Ethereum scarica l'esecuzione su una catena separata.
* Dopo aver elaborato le transazioni, l'altra catena restituisce i risultati da applicare allo stato di Ethereum.

Il vantaggio è che Ethereum non deve eseguire alcuna transazione e deve solo applicare allo stato i risultati dei calcoli esternalizzati. Questo riduce la congestione della rete e migliora anche la velocità delle transazioni (i protocolli off-chain ottimizzano per un'esecuzione più veloce).

La catena ha bisogno di un modo per convalidare le transazioni fuori catena senza rieseguirle, altrimenti si perde il valore dell'esecuzione fuori catena.

È qui che entra in gioco la computazione verificabile. Quando un nodo esegue una transazione al di fuori di Ethereum, presenta una prova a conoscenza zero per dimostrare la correttezza dell'esecuzione fuori catena. Questa prova (chiamata prova di validità – validity proof, in cui le transazioni per alcune soluzioni di livello 2 vengono raggruppate in lotti ed inviate ad Ethereum come singola transazione, effettuando il calcolo al di fuori della catena e portandolo poi su quella principale) garantisce che una transazione è valida, consentendo a Ethereum di applicare il risultato al suo stato, senza aspettare che qualcuno lo contesti.

I rollup a conoscenza zero (zk-rollups) e i validium sono due soluzioni di scalabilità off-chain che utilizzano le prove di validità per fornire una scalabilità sicura. Questi protocolli eseguono migliaia di transazioni fuori dalla catena e inviano le prove di validità per la verifica su Ethereum. I risultati possono essere applicati immediatamente una volta che la prova è stata verificata, consentendo a Ethereum di elaborare un maggior numero di transazioni senza aumentare la computazione sul livello di base.

* Ridurre la corruzione e la collusione nel voto on-chain

I sistemi di voto su blockchain hanno molte caratteristiche favorevoli: sono completamente verificabili, sicuri contro gli attacchi, resistenti alla censura e liberi da vincoli geografici. Ma anche gli schemi di voto on-chain non sono immuni dal problema della collusione.

Definita come "coordinamento per limitare la libera concorrenza ingannando, frodando e fuorviando gli altri", la collusione può assumere la forma di un attore malintenzionato che influenza il voto offrendo tangenti. Ad esempio, Alice potrebbe ricevere una bustarella da Bob per votare l'opzione B in una scheda elettorale anche se preferisce l'opzione A.

La corruzione e la collusione limitano l'efficacia di qualsiasi processo che utilizzi il voto come meccanismo di segnalazione (soprattutto quando gli utenti possono dimostrare come hanno votato). Questo può avere conseguenze significative, soprattutto quando i voti sono responsabili dell'allocazione di risorse scarse.

Ad esempio, i meccanismi di finanziamento quadratico (si apre in una nuova scheda) si basano sulle donazioni per misurare la preferenza per determinate opzioni tra diversi progetti di bene pubblico. Ogni donazione conta come un "voto" per un progetto specifico, e i progetti che ricevono più voti ottengono più fondi dal pool di finanziamento.

L'uso del voto su catena rende il finanziamento quadratico suscettibile alla collusione: le transazioni su blockchain sono pubbliche, quindi i corruttori possono ispezionare l'attività su catena di un beneficiario per vedere come ha "votato". In questo modo il finanziamento quadratico cessa di essere un mezzo efficace per l'allocazione dei fondi in base alle preferenze aggregate della comunità.

Fortunatamente, soluzioni più recenti come MACI (Minimum Anti-Collusion Infrastructure) utilizzano prove a conoscenza zero per rendere le votazioni sulla catena (ad esempio, i meccanismi di finanziamento quadratico) resistenti alla corruzione e alla collusione. Il MACI è un insieme di contratti intelligenti e script che consentono a un amministratore centrale (chiamato "coordinatore") di aggregare i voti e contare i risultati senza rivelare le specifiche su come ogni individuo ha votato. In ogni caso, è possibile verificare che i voti siano stati contati correttamente o confermare che un particolare individuo ha partecipato al turno di votazione.

* Come funziona il MACI con le prove a conoscenza zero?

All'inizio, il coordinatore distribuisce il contratto MACI su Ethereum, dopodiché gli utenti possono iscriversi al voto (registrando la propria chiave pubblica nello smart contract). Gli utenti votano inviando messaggi criptati con la loro chiave pubblica allo smart contract (un voto valido deve essere firmato con la chiave pubblica più recente associata all'identità dell'utente, oltre ad altri criteri). In seguito, il coordinatore elabora tutti i messaggi una volta terminato il periodo di votazione, conta i voti e verifica i risultati sulla catena.

Nel MACI, le prove a conoscenza zero sono utilizzate per garantire la correttezza del calcolo, rendendo impossibile per il coordinatore elaborare in modo errato i voti e il conteggio dei risultati. Ciò si ottiene richiedendo al coordinatore di generare prove ZK-SNARK che verifichino che a) tutti i messaggi sono stati elaborati correttamente b) il risultato finale corrisponde alla somma di tutti i voti validi.

In questo modo, anche senza condividere la ripartizione dei voti per utente (come avviene di solito), il MACI garantisce l'integrità dei risultati calcolati durante il processo di conteggio. Questa caratteristica è utile per ridurre l'efficacia degli schemi di collusione di base. Possiamo esplorare questa possibilità utilizzando l'esempio precedente di Bob che corrompe Alice per farle votare un'opzione:

* Alice si registra per votare inviando la propria chiave pubblica a uno smart contract.
* Alice accetta di votare per l'opzione B in cambio di una tangente da parte di Bob.
* Alice vota per l'opzione B.
* Alice invia segretamente una transazione criptata per cambiare la chiave pubblica associata alla sua identità.
* Alice invia un altro messaggio (criptato) allo smart contract che vota per l'opzione A utilizzando la nuova chiave pubblica.
* Alice mostra a Bob una transazione che mostra che ha votato per l'opzione B (che non è valida poiché la chiave pubblica non è più associata all'identità di Alice nel sistema).
* Durante l'elaborazione dei messaggi, il coordinatore salta il voto di Alice per l'opzione B e conta solo il voto per l'opzione A. Di conseguenza, il tentativo di Bob di colludere con Alice e manipolare il voto sulla catena fallisce.

L'uso del MACI richiede la fiducia nel coordinatore affinché non colluda con i corruttori o tenti di corrompere gli elettori. Il coordinatore può decriptare i messaggi degli utenti (necessari per creare la prova), in modo da poter verificare con precisione come ogni persona ha votato.

* Sicurezza per le informazioni sensibili (informazioni sulla carta di credito)

Le informazioni sensibili, come gli estratti conto o le informazioni della carta di credito, necessitano di un ulteriore livello di protezione. La banca conserva lo storico della carta di credito. Tuttavia, quando si richiedono le informazioni, è necessario comunicare con il loro server.

Anche se le banche utilizzano una linea sicura, la storia della carta di credito è molto più sensibile dei dati medi. In questo caso, non limitandosi a crittografare l'intera informazione in un unico blocco, le banche possono garantire una maggiore sicurezza.

Poiché le banche manipolano solo i blocchi necessari senza toccare altri blocchi, la vostra storia avrà il giusto livello di sicurezza. ZKP è in grado di fornirlo.

* Documentazione complessa

ZKP può impedire a qualsiasi utente di accedere a documentazione complessa che non è autorizzato a vedere. Poiché ZKP è in grado di crittografare i dati in blocchi, sarà sufficiente manipolare alcuni blocchi per consentire l'accesso e limitare l'accesso ad altri utenti. In questo modo, le persone non autorizzate non potranno vedere i vostri documenti.

* Protezione dell'archiviazione

Può fornire una maggiore protezione per l'utilità di archiviazione. ZKP è dotato di un protocollo che tiene lontani gli hacker. In questo modo, non solo l'unità di archiviazione ma anche le informazioni al suo interno saranno crittografate. Inoltre, anche il canale di accesso sarà protetto al massimo.

* Controllo del file system

Tutto ciò che si trova all'interno di un file system può essere protetto dal protocollo zero-knowledge proof. I file, gli utenti e persino ogni login possono avere diversi livelli di sicurezza. Quindi, può essere un ottimo caso d'uso quando necessario.

## Applicazione alla SSI

L’uso combinato delle due tecnologie è particolarmente interessante perché consente di garantire la privacy e la sicurezza delle informazioni personali degli utenti.

* La Self Sovereign Identity si basa sull'idea che gli individui dovrebbero avere il controllo completo delle loro informazioni personali e dovrebbero essere in grado di condividerle solo con le parti che desiderano.
* La tecnologia ZKP può essere utilizzata per garantire la privacy delle informazioni personali degli utenti, consentendo loro di condividere solo le informazioni necessarie senza rivelare il contenuto completo.

Ad esempio, supponiamo che un individuo debba mostrare la sua età per accedere a un servizio online. Utilizzando la tecnologia ZKP, l'individuo può dimostrare di avere un'età superiore a una certa soglia senza rivelare la propria età effettiva. In altre parole, la prova di età viene fornita senza rivelare informazioni personali aggiuntive.

La tecnologia ZKP può anche essere utilizzata per garantire che le informazioni personali degli utenti siano autentiche, senza dover rivelare il contenuto completo. Ad esempio, una persona può dimostrare di essere un cittadino di un determinato paese senza dover rivelare la propria data di nascita o altri dettagli personali.

Inoltre, la tecnologia ZKP può essere utilizzata per garantire la sicurezza delle informazioni personali degli utenti. Ad esempio, se un'organizzazione deve verificare l'identità di un individuo, può farlo senza dover memorizzare le informazioni personali dell'individuo. In questo modo, le informazioni personali degli utenti non possono essere compromesse in caso di violazioni dei dati.

Esiste un'implementazione indipendente di ZKP da parte di ZCash - ZK-SNARK. Si tratta della versione iniziale, successivamente finalizzata dall'implementazione di ZKP per l'identificazione anonima degli utenti nei registri ZK-STARK distribuiti. ZK-STARK accelera significativamente il tempo necessario per creare i registri, elaborare e verificare sia il verificatore che il verificato. Gli studi teorici indicano che ZK-STARK non necessita di calcoli ad alte prestazioni ed è robusto dal punto di vista crittografico anche in caso di cracking da parte di computer quantistici.

Attualmente, sono in fase di sviluppo i seguenti componenti sulla base delle tecnologie DID e ZKP:

* Autenticazione dell'utente;
* Autorizzazione dell'utente;
* Trasferimento dei diritti limitati di un utente a un altro;
* Anonimizzazione dell'utente annidato.

Il meccanismo di interazione DIDs consente di fornire a un utente un accesso limitato alle risorse di un altro. risorse di un altro. In questo caso, l'utente 1 crea una nuova DID, che è una copia della sua verificata DID\_1 per una determinata operazione con funzionalità limitate e lo trasferisce all'utente 2. L'esempio più semplice esempio di tale restrizione può essere un periodo di tempo dopo il quale l'utente 2 non può più utilizzare la sua copia di DID\_1.

Immagine che contiene diagramma

Descrizione generata automaticamente

Riferimento: <https://ceur-ws.org/Vol-2507/381-385-paper-70.pdf>

L’integrazione complementare e successiva delle due tecnologie è standardizzato da parte di Decentralized Identity Foundation (DIF), che sviluppa standard aperti e protocolli per consentire agli utenti di gestire le proprie identità digitali in modo sicuro e privato. DIF supporta anche l'utilizzo di tecnologie come la ZKP per garantire la privacy e la sicurezza delle informazioni personali degli utenti.

Questo può avvenire principalmente tramite due tecnologie:

* Verifiable Credentials (VC), che consente agli utenti di creare e condividere credenziali verificabili in modo sicuro e privato. Le credenziali verificabili sono informazioni personali che sono state verificate da un'autorità affidabile e che possono essere condivise con terze parti solo con il consenso dell'utente. La tecnologia ZKP può essere utilizzata per garantire che le credenziali verificabili siano autentiche senza rivelare il contenuto completo delle informazioni personali dell'utente.
* DID (Decentralized Identifier), che consente agli utenti di creare identificatori decentralizzati per le proprie identità digitali. L'utilizzo di identificatori decentralizzati consente agli utenti di avere maggior controllo sulla propria identità digitale e di evitare la memorizzazione centralizzata delle informazioni personali.

Con la Zero-Knowledge Proof, abbiamo un prover, che è l'individuo, e un verificatore, che deve verificare l'identità di un individuo. In questo caso, tutto ciò che il prover deve mostrare al verificatore è il valore di X, senza mostrare le informazioni reali. Tutto ciò che serve è una prova di conoscenza per verificare che l'individuo sia chi dice di essere. Si tratta di una forma di impronta digitale che può provare l'identità di un individuo. La validità della prova risiede nell'utilizzo di una funzione hash crittografica che dimostra senza ombra di dubbio che l'identità è valida.

Quando si utilizza una funzione di hash su un insieme di dati variabili, come nel caso delle informazioni personali (non sono tutte della stessa lunghezza), l'output può essere costantemente un valore fisso. È qui che sta la verifica, perché la manomissione è altamente improbabile e richiede un'estrema potenza di calcolo o fortuna. Quando i dati sono sottoposti a hashing, gli input non possono essere facilmente determinati in base agli output. Nel caso dell'identità auto-sovrana, le informazioni personali degli individui possono essere memorizzate in un database privato che può anche essere centralizzato sotto il governo. Tuttavia, le informazioni vengono poi sottoposte a hashing e il valore viene memorizzato su un database separato che è pubblico e utilizza una blockchain.

# Sicurezza e vulnerabilità

La sicurezza delle Blockchain richiede l'adozione di diverse metodologie e pratiche provenienti da diverse discipline. Questi includono:

1. Utilizzo del protocollo di sicurezza TLS: Si tratta di un protocollo crittografico che protegge la comunicazione tra i nodi della blockchain, garantendo la confidenzialità e l'integrità dei dati scambiati.

2. Protezione delle transazioni basate su API: È fondamentale implementare meccanismi di sicurezza per proteggere le transazioni effettuate attraverso le API, come l'autenticazione e la crittografia dei dati trasmessi.

3. Implementazione di sistemi di autenticazione multi-fattore: Per aumentare la sicurezza, è consigliabile utilizzare sistemi di autenticazione che richiedono più di un fattore, ad esempio una combinazione di password, token e biometria.

4. Gestione robusta delle chiavi crittografiche: È fondamentale implementare un sistema affidabile per la generazione, l'archiviazione e la gestione delle chiavi crittografiche utilizzate nella blockchain. Questo include l'adozione di pratiche di protezione delle chiavi e il monitoraggio costante per rilevare eventuali anomalie o accessi non autorizzati.

5. Implementazione di protocolli come OAuth, OIDC e SAML2: Questi protocolli standard consentono lo scambio sicuro di autorizzazioni e autenticazioni tra diversi domini. Ad esempio, OAuth consente l'emissione di token da parte di un server per consentire ai client di accedere a determinati servizi. Questi protocolli sono ampiamente utilizzati da grandi aziende come Amazon, Google, Meta (Facebook) e Microsoft per consentire agli utenti di condividere informazioni con altri servizi web in modo sicuro.

La sicurezza del Web3 si basa sulla caratteristica fondamentale delle blockchain di essere resilienti all'intervento umano. Questo significa che una blockchain ben progettata offre una forte garanzia che il codice continuerà a funzionare come previsto, rendendo il sistema informatico autonomo e affidabile.

Tuttavia, la natura irreversibile delle transazioni blockchain rende le reti controllate dal software un obiettivo allettante per gli attaccanti. Con l'aumentare del valore delle blockchain e delle applicazioni ad esse collegate, gli attacchi diventano sempre più sofisticati e mirati, rappresentando veri e propri honeypot da colpire.

Gli attacchi nel mondo delle criptovalute possono essere classificati in base alla loro sofisticatezza, all'automazione e alle contromisure che possono essere adottate per difendersi. Alcune categorie di attacco includono:

1. APT (Advanced Persistent Threats): Questi sono attacchi condotti da gruppi altamente organizzati e persistenti. Alcuni APT si concentrano specificamente su progetti Web3, come il gruppo nordcoreano Lazarus (APT38), che ha condotto l'hacking del bridge Ronin. Questi attacchi sono caratterizzati da un alto livello di sofisticazione e spesso sono sostenuti da risorse statali.

2. Attacchi alla governance: Nel contesto del Web3, molte piattaforme includono meccanismi di governance in cui i possessori di token possono proporre e votare per modifiche all'organizzazione o alla rete. Questo offre opportunità di miglioramento, ma può anche essere sfruttato per attività dannose. Gli attaccanti possono utilizzare tecniche come i flash loan per acquisire un gran numero di token di governance e ottenere il controllo della rete.

3. Attacchi agli oracoli: Gli oracoli forniscono dati real-time sul mondo reale alle blockchain, ma possono essere vulnerabili agli attacchi. Manipolando i dati forniti dagli oracoli, gli aggressori possono influenzare i prezzi degli asset e trarre vantaggio dalla volatilità dei mercati DeFi.

4. Nuove vulnerabilità: Nel Web3, gli exploit zero-day rappresentano una minaccia significativa. Gli attaccanti possono dedicare tempo a esaminare il codice delle DApp per individuare vulnerabilità che possono sfruttare. Alcune vulnerabilità note, come il re-entrance bug, continuano ad affliggere progetti nel mondo Web3 nonostante siano state identificate in passato.

La comunità del Web3 sta investendo nella sicurezza, tra cui audit, monitoraggio e strumenti automatizzati, per affrontare queste minacce. Tuttavia, la valutazione e la correzione di nuove vulnerabilità rappresentano una sfida in continua evoluzione per la comunità.

Altre vulnerabilità importanti altre volte discusse:

* Reentrancy attack – DAO

Il primo attacco di cui parleremo è chiamato "Reentrancy Attack", che sfrutta la mancanza di controlli che dovrebbero avvenire durante il processo di prelievo da un portafoglio.

Immaginate un sistema bancario tradizionale che controlla il nostro saldo solo al momento del login. In questo caso, saremmo in grado di effettuare transazioni per un importo superiore al nostro saldo effettivo perché il controllo del saldo avviene solo a monte.

Il caso più famoso di Reentrancy Attack si è verificato nel 2016 contro The DAO, un fondo di investimento basato su smart contract che effettuava il controllo del saldo dell'utente dopo il trasferimento di Ether. Gli aggressori sono riusciti a rubare circa 70 milioni di dollari.

Per prevenire questo tipo di attacco alla blockchain, è consigliabile limitare la quantità di Ether che può essere prelevata potenzialmente all'infinito.

* Contratto avvelenato (Poison contract)

I contratti intelligenti sono programmi eseguiti sulla blockchain e possono svolgere diverse funzioni, tra cui l'invio e il deposito di criptovalute.

Ogni utente che vuole interagire con uno smart contract deve fornire l'indirizzo del proprio portafoglio o l'indirizzo di uno smart contract autocreato in grado di immagazzinare criptovalute.

Il fatto che gli smart contract permettano ad altri contratti di connettersi tra loro li rende vulnerabili a una serie di problemi di sicurezza, tra cui i contratti avvelenati.

Un contratto avvelenato non "ruba" criptovalute e l'attaccante non ne ricava nulla. È programmato esclusivamente per interrompere il funzionamento del contratto che sta attaccando.

I contratti vulnerabili a questo tipo di attacco hanno funzioni che interagiscono in modo sequenziale con gli utenti, come ad esempio un processo che ridistribuisce automaticamente le vincite del gioco ai partecipanti.

Se un utente utilizza un contratto velenoso durante la distribuzione delle vincite, programmato per consumare un'enorme quantità di gas per raggiungere il limite di blocco, bloccherà l'esecuzione del contratto e, quindi, il pagamento per tutti gli utenti, compreso se stesso.

Questo tipo di attacco rientra nella categoria dei denial of service o DoS, in cui gli aggressori ottengono un vantaggio impedendo a determinati utenti di utilizzare un servizio o di accedere a una risorsa.

* Underflow e overflow di interi

Un'altra vulnerabilità degli smart contract è la presenza dei bug Integer Underflow e Overflow. Quali sono le cause?

I bug di overflow e underflow sono spesso causati da una programmazione poco attenta e dalla mancanza di controlli su variabili numeriche, come un conto bancario o un portafoglio di criptovalute.

In informatica, i computer memorizzano i dati in diversi "tipi": numeri, testo e molti altri. Per quanto riguarda i dati numerici, in realtà esiste un numero infinito di numeri rappresentabili, ma i computer hanno una memoria finita, quindi c'è un limite alle cifre che possono essere rappresentate in un linguaggio di programmazione.

Di conseguenza, cosa succede quando cerchiamo di calcolare un numero troppo grande per la memoria del nostro computer?

Il numero in questione si "avvolge" e torna al numero più piccolo che può rappresentare, cioè zero. Questo fenomeno si chiama overflow dei numeri interi.

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

Riferimento dell’immagine e parti tradotte:

<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjYwM_Xyqv_AhVnMOwKHVLRBEEQFnoECCsQAQ&url=https%3A%2F%2Fdrpress.org%2Fojs%2Findex.php%2FHSET%2Farticle%2Fview%2F5498%2F5317&usg=AOvVaw05p7ZqNd7Hlkhtmpcb8yVm>

* Vulnerabilità di Solidity

1. Errore di tipo intero

Gli errori di tipo intero consistono principalmente in errori di troncamento, errori di segno ed errori aritmetici. Gli errori aritmetici includono l'overflow di un intero, la divisione per zero e il modulo zero. L'EVM utilizza diverse lunghezze fisse per rappresentare i numeri interi, il che significa che può rappresentare solo numeri all'interno di un certo intervallo e che una volta il risultato di una singola operazione sui numeri interi si trova al di fuori di questo intervallo, si può verificare un overflow di numeri interi. Un utente malintenzionato può utilizzare una vulnerabilità di tipo integer overflow per saltare alcuni giudizi condizionali o manomettere i dati, come nel famoso caso della vulnerabilità BEC, in cui si è verificato un overflow di interi durante un trasferimento che ha portato all'evaporazione di un gran numero di token. Le vulnerabilità di overflow possono essere efficacemente evitate utilizzando la libreria di calcolo SafeMath che fornisce controlli di sicurezza.

Nelle versioni precedenti di EVM e Solidity, la divisione per zero e la modulazione di zero comportano solo un'operazione con un risultato pari a zero e nessuna eccezione. Un errore di troncamento è una perdita di precisione causata da conversione di dati di tipo intero in dati di tipo intero con larghezza inferiore. Un errore simbolico è il risultato di un numero negativo diventa un numero intero molto grande e i dati interi firmati della stessa dimensione vengono convertiti in dati interi senza segno della stessa dimensione.

Per affrontare i problemi relativi agli interi, si raccomanda di aggiungere le funzioni require(), funzioni assert() o database SafeMath.sol per eseguire test sulle operazioni aritmetiche. È anche possibile dedicare del tempo a confrontare i simboli e gli argomenti per implementare le operazioni aritmetiche prima che la funzione venga eseguita.

2. Casualità con l'uso di 'Block Hash'

A volte la casualità è necessaria in un'operazione; a questo scopo, è bene usare l'hashing a blocchi Tuttavia, può essere manipolato come un timestamp, i minatori possono prevedere la stessa cosa

Altre transazioni all'interno dello stesso blocco possono facilmente leggere il valore di hash del blocco. Se è un minatore a subire l'attacco, allora la situazione potrebbe peggiorare. Ad esempio, Oracle, RANDAO, RNG e altre risorse esterne casuali.

3. Valore di ritorno non controllato

Anche le chiamate di funzione nel linguaggio Solidity della rete Ethereum impostano il valore di ritorno, ma il fallimento delle chiamate di funzione di basso livello (come ad es.

fallimento delle chiamate di funzione di basso livello (come call, send, delegatecall, ecc.) mostra semplicemente nel valore di ritorno se si è verificata un'eccezione.

Un aggressore potrebbe far sì che il programma venga eseguito in modo diverso da quello di un'operazione fallita, causando così confusione sullo stato dello smart contract. contratto intelligente. Gli sviluppatori possono assicurarsi che un contratto venga eseguito con la logica predefinita controllando il valore di ritorno delle chiamate di funzione di basso livello per determinare se la chiamata è andata a buon fine durante lo sviluppo del contratto.

4. Problema del controllo dei permessi

Le funzioni e le variabili di stato possono essere rese visibili in Solidity utilizzando quattro descrittori: external, internal, public e private. La visibilità non dichiarata è predefinita su public, il che significa che la funzione non solo può essere chiamata internamente, ma anche non solo può essere chiamata internamente, ma anche come interfaccia esterna al contratto. Se una funzione che operazioni sensibili, come i trasferimenti, non viene dichiarata la visibilità, questo potrebbe consentire a un attaccante di approfittare della situazione.

5. Denial-of-Service (DoS)

Per Denial-of-Service (DoS) si intende un'operazione che non può essere recuperata o un consumo controllato di risorse illimitate. Un attacco DoS contro un contratto di Ether può portare a una massiccia di Ether e Gas o, nei casi più gravi, la perdita permanente dell'uso del contratto.

6. Chiamata all'ignoto

Quando le funzioni di fallback sono state eseguite in determinate condizioni e la firma della funzione non è vera. La funzione che ha portato all'utilizzo del contratto Calle, attraverso un altro smart contract, sarà implementata nel trasferimento di Ethereum. Per migliorare la sicurezza della chiamata a funzioni e contratti sconosciuti, l'ultimo compito del codice locale è quello di effettuare una chiamata alla funzione sconosciuta. Il modello di interazione a effetto deve essere utilizzato per prevenire cambiamenti di stato dopo la chiamata di un contratto sconosciuto.

7. Invio senza gas

Ogni contratto smart Ether richiede il pagamento di una tassa sul gas quando l'Ether viene trasferito nel contratto quando questo entra in vigore. L'eccezione out-of-gas verrà lanciata quando il gas massimo per la funzione di fallback in un contratto Calle è di 2300. Un utente malintenzionato potrebbe sfruttare questa vulnerabilità per trarre profitto conservando gli Ether non trasferiti a causa dell'eccezione.

La funzione di fallback per la gestione delle eccezioni per la gestione delle eccezioni dovute a un errore nel consumo di gas dovrebbe rendere l'esecuzione meno costosa, mitigando i fallimenti del contratto e i costi.

8. Griefing del gas insufficiente

I dati esterni utilizzano lo stesso contratto nella sottocall, vulnerabile agli attacchi di gas griefing quando la subcall fallisce, l'intero processo può essere completamente recuperato. Quindi, gli hacker possono impedire che la subcall fallisca per censurare le transazioni. Per evitare che ciò accada, la creazione di una funzione dovrebbe verificare se fornisce abbastanza unità di gas o meno. Inoltre, è utile consentire a un estraneo fidato di rivedere e premiare le transazioni andate a buon fine.

9. Collisione di hash con gli argomenti

abi.encodePacked() è uno schema di impacchettamento non standard, utilizzato principalmente per indicizzare i parametri di impacchettamento. Quando ci sono molti parametri di dimensioni variabili, in alcuni casi 'abi.encodePacked()' in fase di esecuzione può causare un conflitto di hash. Questo schema di impacchettamento impacchetta i parametri in modo sequenziale, indipendentemente dall'ordine dei parametri e gli hacker sono in grado di cambiare la posizione dei parametri per verificare la firma. Si raccomanda di usare "abi.encode()" per inoltrare i parametri e, quando si passano i parametri, solo array a lunghezza fissa o parametri singoli.

* Caratteristiche della macchina virtuale Ethereum (EVM)

1. Rientro

Quando un utente chiama uno smart contract, chiama un fallback se il contratto chiamato non trova la funzione che dovrebbe essere chiamata o se il contratto accetta solo Ethereum e nessun'altra informazione. che dovrebbe essere chiamata o se il contratto accetta solo Ethereum e nessun'altra informazione. Un utente malintenzionato può costruire una speciale funzione di fallback per attaccare uno smart contract vulnerabile al rientro, come ad esempio una funzione di fallback che contenga codice che contiene codice che richiama una funzione del contratto attaccato che ha precedentemente trasferito denaro all'attaccante, consentendo così chiamate ricorsive ed esaurendo le risorse dell'utente che detiene il contratto. L'evento DAO che ha notoriamente portato all'hard fork di Ether è stato collegato a una vulnerabilità di rientro.

2. Attacco agli indirizzi brevi

Un input utente non controllato è l'attacco Short Address. Un utente malintenzionato utilizza il meccanismo di autocompletamento della VM per costruire un indirizzo con uno zero alla fine per una chiamata a contratto e omette intenzionalmente lo zero nell'indirizzo, che si trova alla fine, per poi passare i parametri. Questo significa che l'importo lasciato sarà raddoppiato, con il risultato che verranno trasferiti più soldi di quelli originariamente impostati. Rilevare gli indirizzi degli utenti e verificare le identità, rifiutare l'input di formati errati, gli attacchi agli indirizzi brevi possono essere evitati.

3. Iniezione di codice

Il meccanismo di delegate call di Ether, che utilizza una direttiva delegatecall che permette ai contratti di eseguire codice di altri contratti nel proprio contesto. Un utente malintenzionato potrebbe sfruttare questa vulnerabilità per iniettare codice in un contratto che modifica operazioni dannose come importanti variabili di stato nel contratto

4. Bug o errori immutabili

Questa è la natura della blockchain di Ethereum, dove una volta implementato un contratto, questo non verrà più modificato e gli errori nel contratto rimangono immutabili e creano alcuni problemi. Per rendere il contratto modificabile in qualsiasi momento, Marino et al. hanno suggerito di affrontare il problema dal punto di vista di uno smart contract, ridefinendo il contratto.

* Caratteristiche di progettazione di Ethereum Blockchain (EBD)

1. Dipendenza dall'ordine di negoziazione

L'ordine di esecuzione di due transazioni dello stesso smart contract può portare a questa vulnerabilità. Gli hacker possono utilizzare questa vulnerabilità per attaccare gli utenti che eseguono modifiche alle transazioni. L'ordine delle transazioni è determinato dai minatori e se i minatori sono hacker, ci sono gravi conseguenze. Per prevenire un attacco di questo tipo, è possibile utilizzare funzioni basate su Ethereum per dettare l'ordine di esecuzione delle transazioni o i termini del contratto suggeriti da Luu et al. “Il codice del contratto o restituisce l'output previsto o fallisce".

2. Dipendenza dal timestamp

Quando il trigger per l'esecuzione di una transazione è il timestamp di un blocco, può portare a una situazione di vulnerabilità in quanto i minatori scorretti possono sfruttare il timestamp del blocco per trattare gli altri. Alcuni contratti intelligenti possono ottenere il timestamp del blocco corrente e utilizzarlo come base di giudizio tramite il parametro block.timestamp, mentre il timestamp può essere determinato dal miner entro certi limiti. Pertanto, è generalmente considerato sicuro utilizzare i timestamp in uno smart contract se il codice dipendente dal timestamp consente un errore di 12 minuti. Poiché i numeri di blocco non possono essere modificati, Luu et al. ritengono che l'uso dei timestamp renderebbe più sicuro per gli hacker, e che le variabili negli smart contract non siano preferibilmente timestamp

3. Mancanza di privacy transazionale

A causa della natura della DeFi, le informazioni sulle transazioni dell'utente sono pubbliche. Molte persone non vogliono essere monitorate, il che limiterà le transazioni degli utenti e minaccerà la privacy e la sicurezza degli stessi.

È una buona scelta criptare il contratto prima che venga distribuito [10] o utilizzare uno strumento [11] per criptare il contratto. Tutte le blockchain dello stesso tipo possono utilizzare questo contratto che preserva la privacy. Il framework di smart contratto intelligente Hawk non può memorizzare alcuna transazione finanziaria, il che rappresenta un'ottima protezione per gli utenti.

4. Elaborazione casuale prevedibile

Alcuni smart contract richiedono fonti di dati esterne, ma se i dati esterni non sono corretti, il contratto fallisce e la correttezza del contratto non è garantita. Un autenticatore è necessario per esaminare i dati esterni e utilizzare dati crittografati.

# Finanziamenti e consorzi coinvolti

La blockchain e i suoi concetti sono stati standardizzati da ISO e IEEE attraverso varie attività, comitati e gruppi di lavoro che si concentrano su diversi aspetti della tecnologia blockchain. L'Organizzazione internazionale per la standardizzazione (ISO) e l'Institute of Electrical and Electronics Engineers (IEEE) hanno collaborato per creare e perfezionare gli standard per le tecnologie blockchain e distributed ledger (DLT).

* ISO/TC 307: Blockchain and distributed ledger technologies è un comitato tecnico dell'ISO che si occupa di vari aspetti della standardizzazione della blockchain, tra cui l'architettura di riferimento, la tassonomia e l'ontologia, la sicurezza informatica, l'identità, i casi d'uso e l'interoperabilità. Il comitato ha pubblicato diversi rapporti tecnici, come l'ISO 22739:2020, che fornisce la terminologia fondamentale per blockchain e DLT.

La standardizzazione di blockchain è presente grazie a ISO 22739:2020, che ha cercato di standardizzare i termini blockchain, tra cui:

- Blockchain: Un libro mastro distribuito con blocchi confermati organizzati in una catena sequenziale di sole appendici che utilizza collegamenti crittografici. Le blockchain sono progettate per essere resistenti alle manomissioni e creare registri finali, definitivi e immutabili.

- Sistema decentralizzato: Un sistema in cui il controllo è distribuito tra le persone o le organizzazioni che partecipano al funzionamento del sistema [Fonte 3](https://medium.com/reale/ui/#!iso:std:ui:eefbc8a8-0fcf-4933-8055-5a8e882cc2ad/iso-22739-2020).

- Oracolo DLT: Un servizio che aggiorna un libro mastro distribuito utilizzando dati provenienti dall'esterno di un sistema DLT, utile per gli smart contract che non possono accedere a fonti di dati esterne al sistema DLT.

- Immutabilità: Una proprietà per cui i record del libro mastro non possono essere modificati o rimossi una volta aggiunti a un libro mastro distribuito.

- Interoperabilità: La capacità di due o più sistemi o applicazioni di scambiarsi informazioni e di utilizzare reciprocamente le informazioni scambiate.

- Fiducia: Il grado di fiducia di un utente o di un'altra parte interessata nel fatto che un prodotto o un sistema si comporterà come previsto da quell'utente o da quell'altra parte interessata.

Fornendo un linguaggio comune per questi termini, la norma ISO 22739:2020 mira a risolvere la confusione e a facilitare la comunicazione all'interno della comunità blockchain e DLT. Questo standard è essenziale per accademici, architetti di soluzioni, clienti, utenti, sviluppatori di strumenti, autorità di regolamentazione, revisori e organizzazioni di sviluppo degli standard.

Similmente, anche il governo italiano ha dato una sua definizione di alcuni termini chiave:

Registro Distribuito (art. 8 ter, 1 comma, L. 12/2019);

Smart Contract (art. 8 ter, 2 comma, L. 12/2019);

La memorizzazione di un documento informatico attraverso l’uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all’articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo del Consiglio, del 23 luglio 2014 (art. 8 ter, 3 e 4 comma, L. 12/2019);

Trattamento Dati Personali (art. 3, Reg. UE 2016/679);

Questi sono soltanto alcuni termini attualmente definiti; spetta a Noi adesso, dimostrare quanto questa tecnologia, inizialmente usata per minare Bitcoin, possa essere il principio cardine della digitalizzazione dei processi aziendali.

L'IEEE, invece, ha istituito la IEEE Blockchain Initiative e l'IEEE Computer Society Blockchain and Distributed Ledgers (BDL) Standards Committee per lavorare sulla standardizzazione della blockchain. L'iniziativa e il comitato per gli standard si concentrano sullo sviluppo di standard per la gestione degli asset digitali basati su blockchain, la classificazione degli asset digitali, i modelli di scambio degli asset digitali, la gestione delle chiavi di identità blockchain e i framework dei sistemi di identità digitale.

L'IEEE ha anche sviluppato standard orizzontali e verticali per le blockchain attraverso il gruppo di lavoro "Blockchain", che si occupa dell'interoperabilità delle blockchain, della denominazione, della coerenza delle transazioni tra le catene, dell'autenticazione dei dati e dei protocolli di comunicazione. Alcuni degli standard sviluppati da IEEE includono IEEE P2418.1 per il quadro di riferimento dell'uso della blockchain nell'IoT e IEEE P2418.2 per i formati di dati standard per i sistemi blockchain.

In sintesi, la standardizzazione della blockchain e dei suoi concetti da parte di ISO e IEEE coinvolge diverse attività, comitati e gruppi di lavoro che si concentrano su diversi aspetti della tecnologia. Queste organizzazioni collaborano per creare e perfezionare gli standard che affrontano vari aspetti della blockchain e della DLT, garantendone il continuo sviluppo e l'adozione.

Parliamo del Consorzio R3 è un gruppo di istituzioni finanziarie che collaborano a iniziative di tecnologia blockchain per migliorare l'infrastruttura dei servizi finanziari. È stato fondato per sviluppare Corda, una piattaforma blockchain progettata specificamente per il settore finanziario. Il consorzio mira a risparmiare denaro, a ridurre gli errori nelle transazioni e ad aumentare significativamente la velocità di liquidazione.

L'ecosistema blockchain di R3 collega una rete eterogenea di aziende del settore pubblico e privato, consentendo agli utenti di scambiare valore attraverso diverse reti Corda con privacy, sicurezza e controllo. Il consorzio ha attirato importanti istituzioni, società fintech e comunità finanziarie fin dal suo inizio.

Corda, l'iniziativa del Consorzio R3, si differenzia da altre soluzioni blockchain finanziarie perché si concentra su privacy, sicurezza e scalabilità. Consente ai partecipanti di condividere i dati delle transazioni solo con chi ne ha bisogno, riducendo il rischio di violazione dei dati e garantendo la conformità alle normative.

Il Consorzio R3 conta più di 40 membri, tra cui importanti banche come HSBC, Deutsche Bank, Citi, Bank of America, Morgan Stanley, Commerzbank, Societe Generale, SEB, BNY Mellon, Mitsubishi UFJ Financial Group, National Australia Bank, Royal Bank of Canada e Toronto-Dominion Bank. Il consorzio è guidato da David Rutter, già CEO del trading elettronico presso ICAP Electronic Trading, mentre il CTO è Richard Brown, proveniente da IBM.

Riguardo al *progetto Corda*, il nome deriva da due fonti, ha dichiarato a Bloomberg Richard Brown, Chief Technology Officer di R3. La prima parte del nome suona come "accordo". La seconda parte deriva dalla definizione di corda, la linea retta più breve tra due punti di un cerchio. Il cerchio rappresenta le banche che compongono la rete R3.

R3 Corda utilizza un approccio alla DLT di tipo "shared ledger", ovvero non esiste un database centrale a cui tutti gli utenti devono collegarsi. Invece, ogni utente ha una copia del libro mastro che tiene aggiornata con le ultime transazioni.

Quando si verifica una transazione, questa viene condivisa solo con le parti coinvolte, garantendo che i dati sensibili rimangano privati e riservati. Una volta che tutte le parti coinvolte nella transazione l'hanno verificata e approvata, questa viene aggiunta al libro mastro di ciascun utente.

Questo approccio presenta diversi vantaggi rispetto ad altre piattaforme DLT, come la blockchain di Bitcoin:

* Riduce in modo significativo la quantità di dati che devono essere memorizzati ed elaborati.
* Rende molto più difficile per i malintenzionati manomettere o cancellare i dati.
* Permette un controllo molto più granulare su chi ha accesso a quali dati.

R3 Corda utilizza anche gli "smart contract" per automatizzare alcuni aspetti delle transazioni. Un contratto intelligente è un pezzo di codice che definisce i termini di un accordo tra due parti. Una volta che tutte le parti hanno accettato i termini del contratto, il codice viene eseguito automaticamente. In altre parole, i processi manuali, come le pratiche e le firme, possono essere sostituiti da processi automatizzati.

I contratti intelligenti possono essere utilizzati per un'ampia gamma di transazioni, da quelle più semplici come il trasferimento di denaro da un conto a un altro a quelle più complesse come l'emissione di obbligazioni o prestiti sindacati.

Le caratteristiche principali di Corda come segue:

* Nessuna condivisione globale non necessaria di dati: solo le parti con una legittima necessità di sapere possono vedere i dati all'interno di un accordo.
* Corda coreografa il flusso di lavoro tra le aziende senza un controllore centrale
* Corda raggiunge il consenso a livello di singoli accordi tra imprese, non a livello di sistema.
* Il design abilita direttamente i nodi di osservazione di vigilanza e regolamentazione
* Le transazioni sono convalidate dalle parti della transazione, piuttosto che da un pool più ampio di validatori non correlati.
* Supporta una varietà di meccanismi di consenso
* Registra un collegamento esplicito tra il codice degli smart contract e i documenti legali in linguaggio umano.
* È costruito su strumenti standard del settore
* Non ha una criptovaluta nativa.

Quando il codice sarà ulteriormente maturato, Corda sarà open source.

I fatti condivisi tra le istituzioni finanziarie includono il seguente tipo di accordo:

* La banca A e la banca B concordano che la banca A deve un certo importo alla banca B, rimborsabile tramite RTGS su richiesta.
* Si tratta di un deposito a vista in contanti
* La Banca A e la Banca B concordano di essere parti di un credit default swap con determinate caratteristiche.
* Si tratta di un contratto derivato
* La Banca A e la Banca B concordano che la Banca A deve consegnare un numero X di unità di una certa azione ordinaria alla Banca B tra tre giorni in cambio di un determinato pagamento in contanti.
* Si tratta di un contratto di consegna contro pagamento

L'industria finanziaria è definita da accordi tra imprese che condividono un problema comune. Entrambe le parti registrano l'accordo in sistemi diversi. La necessità di sistemare le cose quando i diversi sistemi finiscono per credere a cose diverse comporta costi elevati. Ogni anno si spendono decine di miliardi di dollari per questo problema.

I sistemi di solito comunicano scambiandosi messaggi. Molte risorse vengono spese per la riconciliazione, per assicurarsi che le parti siano giunte alle stesse conclusioni.

Brown vede la necessità di un sistema per registrare e gestire gli accordi finanziari condivisi tra le imprese, un accordo che sia visibile alle autorità di regolamentazione necessarie e costruito con strumenti standard del settore.

Il sistema si concentrerebbe sull'interoperabilità e sull'implementazione incrementale, senza rilasciare informazioni riservate a terzi. Un'azienda potrebbe esaminare una serie di accordi con una controparte ed essere certa che ciò che l'azienda vede è ciò che vede anche la controparte e che viene comunicato all'autorità di regolamentazione.

Corda contiene le caratteristiche di consenso, validità, unicità, immutabilità e autenticazione. Brown ha sottolineato che Corda non sta costruendo una blockchain. Il punto di partenza sono gli accordi individuali tra le aziende.

Altra importante iniziativa è Horizon 2020 è un programma di finanziamento pluriennale dell'UE volto a sostenere e incoraggiare i progetti di ricerca dal 2014 al 2020, con un budget totale di quasi 80 miliardi di euro. Si tratta del più grande programma quadro di ricerca e innovazione nella storia dell'UE. Blockchain e Distributed Ledger Technologies (DLT) sono state al centro di numerosi progetti finanziati nell'ambito di Horizon 2020. Progetti degni di nota sono:

* Kedeon: Kedeon è una piattaforma di supply chain basata su blockchain che si concentra sulla fornitura di una soluzione trasparente, sicura ed efficiente per la gestione della supply chain. Sfrutta la tecnologia blockchain per creare un registro decentralizzato e a prova di manomissione delle informazioni sui prodotti, a cui possono accedere e verificare tutti i partecipanti alla catena di approvvigionamento. Questo progetto mira a migliorare la tracciabilità e la responsabilità dei prodotti, garantendone la qualità e l'origine.
* Vestigia: Vestigia è una soluzione basata su blockchain che si concentra sulla fornitura di una catena di approvvigionamento trasparente e sostenibile per l'industria tessile. Utilizza la tecnologia blockchain per creare un registro sicuro e a prova di manomissione della catena di fornitura tessile, comprese le informazioni sui materiali, i processi di produzione e le certificazioni. Questo progetto mira a migliorare la trasparenza, la tracciabilità e la sostenibilità dell'industria tessile.
* Motoblockchain: Motoblockchain è una piattaforma basata sulla blockchain che mette in contatto acquirenti e venditori di moto usate. Utilizza la tecnologia blockchain per creare un registro sicuro, trasparente e verificabile delle informazioni sulle moto, compresa la loro storia, i registri di manutenzione e la proprietà. Questo progetto mira a migliorare la fiducia tra acquirenti e venditori, garantendo la qualità e l'autenticità delle moto usate. Inoltre, le azioni INNOSUP hanno finanziato cinque progetti a sostegno delle PMI nell'adozione di blockchain e DLT, per un totale di circa 10 milioni di euro spesi, di cui 5,1 milioni destinati alle PMI. Questi progetti hanno ricevuto più di 1.100 domande e hanno selezionato oltre 300 PMI e casi d'uso che utilizzano blockchain e DLT.

La Commissione europea ha inoltre istituito un Osservatorio e un Forum Blockchain dell'UE per promuovere l'uso della tecnologia blockchain in vari settori.

Oltre a Horizon 2020, il nuovo programma di finanziamento Horizon Europe dovrebbe continuare a sostenere la ricerca e l'innovazione nella tecnologia blockchain. Si prevede un budget significativo nel seguito del programma Horizon.

Horizon 2020 prevede altri progetti blockchain, come l'azione European Blockchain Pre-Commercial Procurement (PCP), che ha ricevuto 7 milioni di euro di finanziamenti dalla Commissione europea. Il Meccanismo per collegare l'Europa (Connecting Europe Facility, CEF) finanzia l'implementazione dell'infrastruttura di servizi blockchain dell'UE, compresi i casi d'uso concordati nell'ambito del partenariato blockchain dell'UE (EBP).

Inoltre, la Commissione europea sostiene gli investimenti nelle startup e nei progetti blockchain attraverso il nuovo fondo AI & Blockchain Investment, che investe in fondi di venture capital destinati alle startup AI e blockchain, alle imprese in fase iniziale e alle scale-up (startup sviluppate e che puntano a raggiungere il mercato internazionale).

Inoltre, l'UE ha istituito una Giornata informativa su Blockchain, Distributed Ledger Technologies e Fintech di Horizon 2020, con l'obiettivo di illustrare i diversi temi legati alla blockchain e alle tecnologie di distributed ledger nel programma di lavoro di Horizon 2020.

Una collezione di progetti:

* <https://digital-strategy.ec.europa.eu/en/news/overview-eu-funded-blockchain-related-projects>

# 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/>
* VSkills: <https://www.vskills.in/certification/blog/>
* Appinventiv: <https://appinventiv.com/blog/>
* Gataca.io: <https://gataca.io/blog/>
* HolaCripto: <https://www.hola-cripto.com/>
* Simplilearn: <https://www.simplilearn.com/>
* Blocktrade: <https://blocktrade.com/>
* CyberScrilla: <https://cyberscrilla.com>
* 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/>
* Vitalik.ca: <https://vitalik.ca/>
* Ethereum Improvement Proposals: <https://eips.ethereum.org/EIPS/>
* OriginStamp: <https://originstamp.com/blog/>
* GeeksforGeeks: <https://www.geeksforgeeks.org/>
* One37PM: <https://www.one37pm.com/nft/>
* LeewayHertz: <https://www.leewayhertz.com/>
* Hedera: <https://hedera.com/learning/>
* Dock.io: <https://www.dock.io/post/>
* The Motley Fool: <https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/>
* Blog Medium
  + <https://jimmysong.medium.com/>
  + <https://medium.com/coinmonks/>
  + <https://marcomanoppo.medium.com/>
  + <https://ancapalex.medium.com/>
  + <https://unibrightio.medium.com/>
  + <https://medium.com/digitalbitsorg/>
  + <https://medium.com/coinmonks/>
  + <https://medium.com/techskill-brew/>
  + <https://medium.com/metadium/>
* Canali YouTube:
  + <https://www.youtube.com/@DappUniversity>
* Tesi di riferimento:
  + <https://amslaurea.unibo.it/7934/1/bertani_beatrice_tesi.pdf>
* Documenti di riferimento:
  + <https://www.eublockchainforum.eu/sites/default/files/reports/SmartContractsReport_Final.pdf>
  + <https://www.dmi.unict.it/tramonta/sdm/L16_Ethereum.pdf>
  + <https://associazioneblockchain.it/wp-content/uploads/2020/03/20.04.15-I-token.-Una-prospettiva-giuridica.pdf>
* Libri di riferimento:
  + <https://hacken-3.gitbook.io/l1-security/>
  + <https://tokens-economy.gitbook.io/>