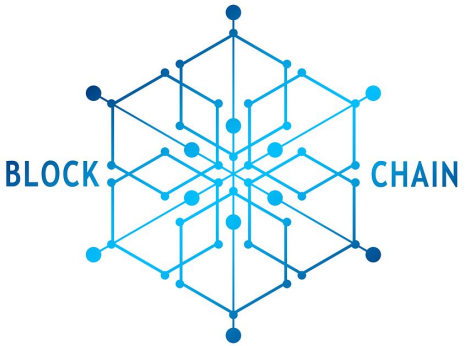
humanativa
CONOSCERE PER INNOVARE

hn BLOCKCHAIN

Modelli di blockchain



I modelli principali di blockchain si possono dividere in:

- blockchain pubbliche
- blockchain private
- DLT - distributed ledger technology

Le reti pubbliche solitamente sono costituite da sistemi P2P dove non ci sono censori, ne controllori, e dove chiunque può sfruttare il network liberamente ed in completa autonomia. Le reti private sono solitamente controllate e gestite in modo centralizzato, da persone, aziende o consorzi.

Mentre i ledger distribuiti possono avere forme diverse, e spesso possono trattarsi anche in fondo solamente di database.

Le blockchain pubbliche, nate tutte con l'ideazione e la realizzazione di Bitcoin, hanno dei vantaggi e degli svantaggi. Propongono come nel caso di Bitcoin, un sistema monetario più equo e libero, ma soffrono di problemi di scalabilità e velocità nelle transazioni.

Questo soprattutto per le blockchain che utilizzano il tipo di consenso tra i nodi detto Proof of Work (PoW). Altri tipi di consenso, come ad esempio Proof of Stake (PoS) permettono elevata velocità ma tendono ad avvicinarsi di più a delle reti private, e forniscono maggior superficie di attacco.

Blockchain private

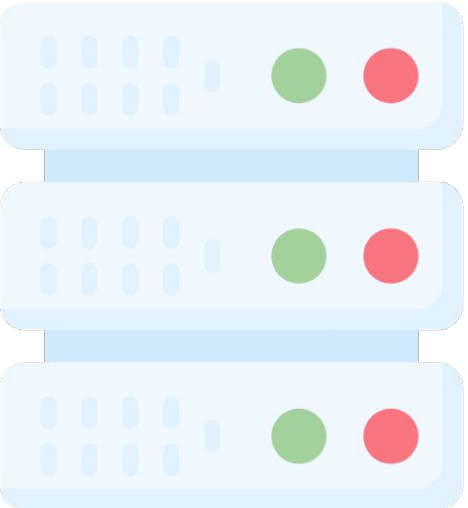
Maggior confidenzialità, più velocità ma meno resilienza agli attacchi

Le **blockchain private** sono solitamente sistemi che si basano su **copie e/o emulazioni** del codice delle **blockchain pubbliche**, ma che vengono **limitate ad un numero di "nodi noti"**, ad una federazione di nodi ad esempio, ed **arricchite** di **sistemi crittografici** per **mantenere i dati riservati** e **non pubblici**.

Sono tipicamente **più veloci**, ma **maggiormente esposte** ad **attacchi informatici**.

Vedremo nelle slide successive:

- Liquid
- Quorum

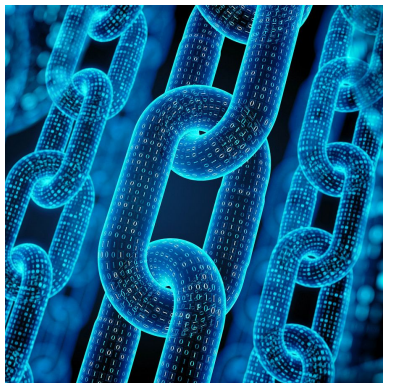


I ledger distribuiti solitamente non fanno uso di una blockchain vera e propria ma utilizzando database tradizionali. Aggiungendo sistemi di distribuzione, di crittografia asimmetrica e firma digitale semplice, hash, crittografia simmetrica e a volte crittografia omomorfica.

Nelle slide seguenti vedremo alcuni esempi di DLT,
i più noti sono:

- Corda
- Hyperledger

“Blockchain pubbliche”



Rispetto alle blockchain private il network Bitcoin ha dei **limiti di scalabilità**, attualmente **in risoluzione** tramite il **Layer 2** lightning network, ed una **trasparenza completa**. Non permette infatti ne scambio di dati e transazioni da punto a punto ne l'anonimicità di importi ed indirizzi.

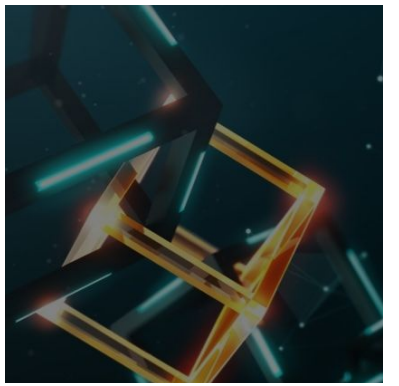
Tuttavia rappresenta la **rete** al momento **più difficile** da **attaccare** e quindi di fatto la **più immutabile**.

Nasce con lo **scopo** di fornire in tutto il mondo una **rete di pagamento** ed un **nuovo tipo di denaro**, in modalità **P2P** quindi **senza censure**, e **senza autorizzazioni** per l'utilizzo, ed inoltre **non richiede** l'intervento di **terze parti** per lo scambio di transazioni.

Su oltre 2000 brutte copie di Bitcoin, nate dal suo codice open source, **Ethereum è una delle poche blockchain** e criptovalute che ha avuto il **merito di portare un innovazione**. I **nodi** della rete Ethereum hanno una **VM** specifica che permette di far girare **codice turin complete** e quindi di **poter scrivere smart contract** molto più complessi di quelli disponibili su Bitcoin.

Al momento Ethereum soffre molto, anche più di Bitcoin, dei problemi di scalabilità tipici delle blockchain pubbliche.

“Blockchain private”



Liquid è un prodotto di BlockStream una delle più importanti società che opera su Bitcoin e blockchain. Per molto tempo leader nel settore, ha raccolto moltissimi degli sviluppatori “Core” di Bitcoin.

Liquid rappresenta una soluzione ai problemi di scalabilità della blockchain di Bitcoin. Si tratta di una **blockchain privata** composta da **21 nodi federati**, che ha una **velocità di transazione ottimale**, e che permette di gestire anche sotto asset oltre al BTC, offrendo quindi **funzionalità per la tokenizzazione**. Una **soluzione** attualmente in particolare **adottata** da diversi servizi di **exchange di cripto valute** per velocizzare le transazioni.

Quorum

Quorum è una blockchain privata sviluppata da team tecnico di **JPMorgan** Chase, **ottenuta modificando la sorgente open source della rete Ethereum**. Questo la rende più **facilmente integrabile** con la **rete** pubblica di **Ethereum** stessa.

Il prodotto presenta tutte le funzionalità di Ethereum, stesso linguaggio di programmazione per scrivere smart contract, ma aggiunge un **layer di crittografia** per **rendere private le transazioni** e le informazioni degli smart contract ad un **sottoinsieme di nodi** della rete.

Tra i vari attori EY sta spingendo molto su questa tecnologia, sfruttando un utilizzo combinato di reti private basate su Quorum che poi **notarizzano continuamente** informazioni **sulla rete** pubblica di **Ethereum** per **aggiungere** maggior **sicurezza**.

“DLT - distributed ledger technology”

Quantum Ledger Database è un servizio offerto da **Amazon** che garantisce la disponibilità in cloud di un “Diario di appendice” **immutabile e trasparente**. Fornendo una memorizzazione precisa e sequenziata di ogni modifica di un dato.

Il servizio a livello commerciale non cerca di proporsi come una blockchain, ma semplicemente come un database dove i dati non possono essere cancellati e sono firmati crittograficamente e storicizzati.

Risponde quindi alle **esigenze** di **storicizzazione, immutabilità, trasparenza e certificazione dei dati**.

HYPERLEDGER
FABRIC

HyperLedger Fabric è un **prodotto open source** della **Linux foundation**, i primi a collaborare alla sua scrittura sono stati Blockstream e IBM e successivamente INTEL. Oggi **la governance** del progetto è ripartita tra **molte grandi aziende** e **consorzi** IT e blockchain.

HyperLedger offre un **sofisticato sistema di permessi**, fornendo l'**accesso** ai **dati** del ledger anche a **piccole porzioni** dei **partecipanti** della rete.

L'**applicazione** più **interessante** attualmente in corso su questa tecnologia rappresenta il tracciamento della supply chain, grazie ad una partnership tra IBM e Maersk da cui nasce il progetto Tradelens.

Corda, ed il Corda Network è un prodotto che fornisce un **ledger distribuito**, non basato su blockchain ma su **database relazionale**, e classi in **Java** per la gestione di **transazioni** private, riguardanti dati o asset, **da punto a punto** e non broadcast tra i vari nodi.

Principalmente **usato da banche** e aziende che forniscono servizi alle banche. Corda intende fornire una **soluzione ai problemi di scalabilità** delle blockchain, aggiungendo un concetto di **riservatezza "by default" delle transazioni**.

I network più noti basati su questa tecnologia sono **Corda R3** e **SIAChain**, quest'ultima è il primo esempio di applicazione di corda con una CA indipendente da Corda R3.

humanativa

CONOSCERE PER INNOVARE

Humanativa Group S.p.A.

Sede Legale ed Operativa

Viale della Grande Muraglia, 284 · 00144 Roma · Tel. +39.06.89161268 · Fax +39.06.89161316

Sede Operativa

Via Gian Domenico Romagnosi, 11A · 00196 Roma · Tel. +39.06.36002917

Formazione

Via XX Settembre, 98e · 00187 Roma

Sede di Milano

Piazza Armando Diaz, 1 · 20123 Milano

www.humanativaspa.it · info@humanativaspa.it