

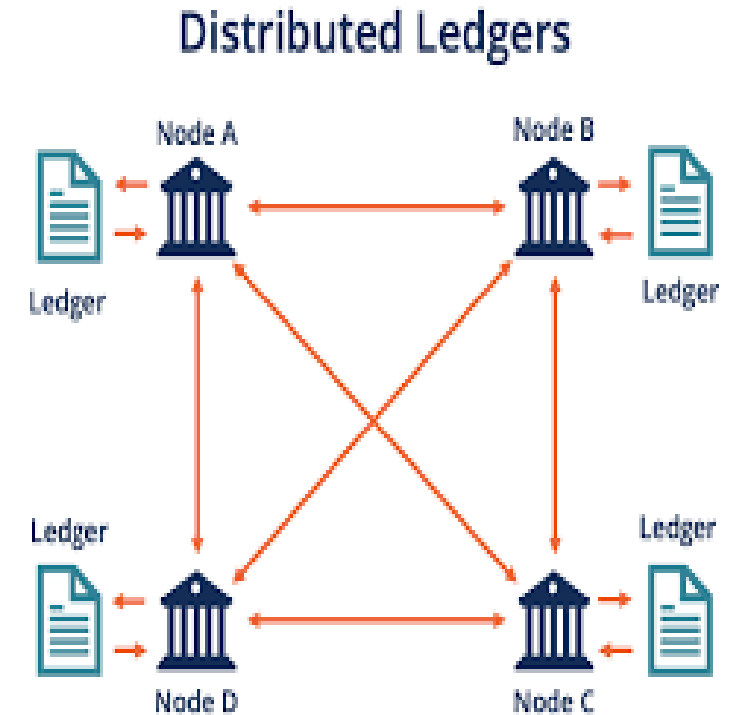
Distributed Ledger Technology

Francesco Pugliese, PhD

neural1977@gmail.com

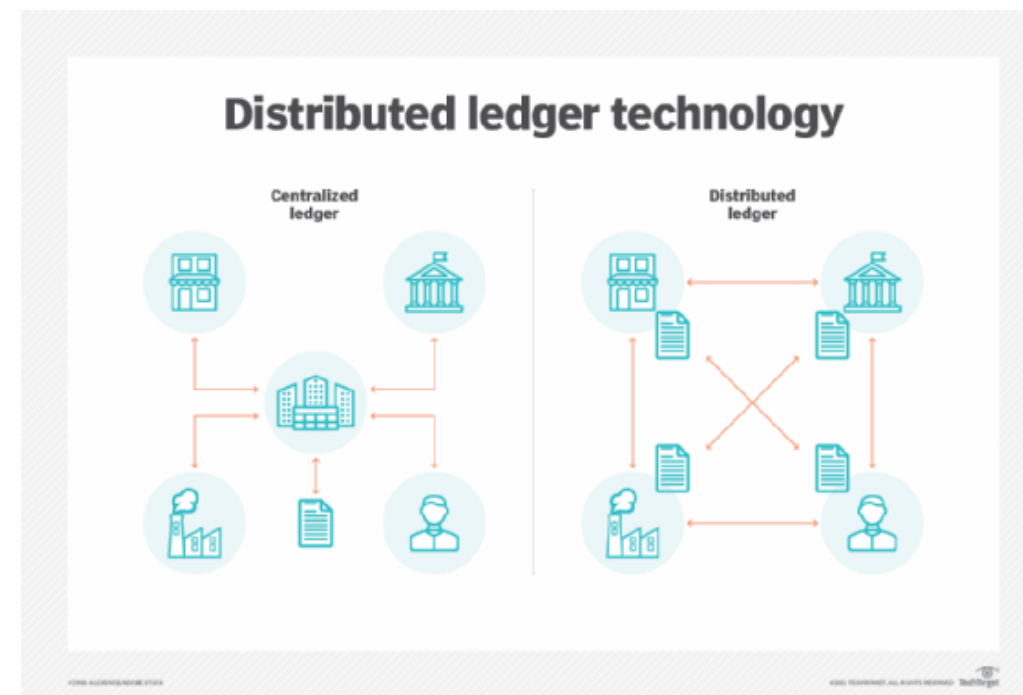
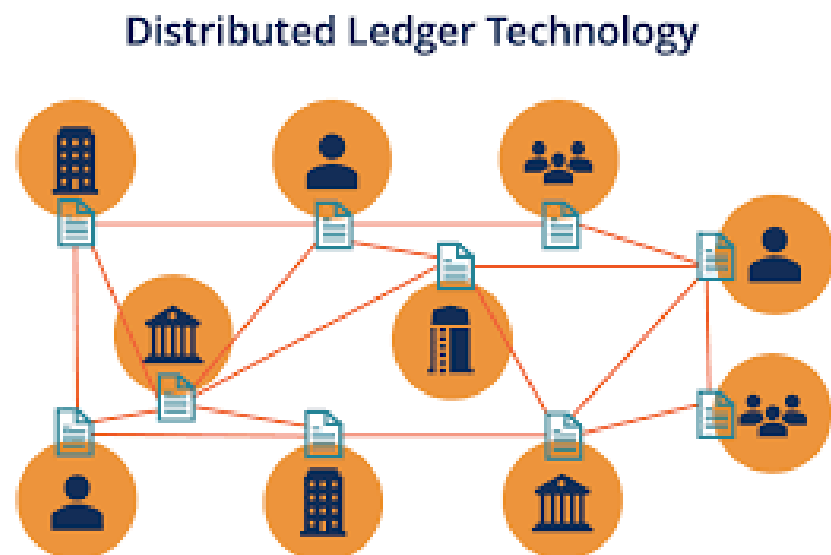
Distributed Ledger Technology

- ✓ Le tecnologie **Distributed Ledger (DLT)** sono sistemi basati su un registro distribuito, e a questa grande famiglia appartiene anche la **Blockchain**. Sono sistemi basati su un **registro distribuito**, ossia sistemi in cui tutti i nodi di una rete possiedono la stessa copia di un database che può essere letto e modificato in modo indipendente dai singoli nodi.
- ✓ Se tutti che possiedono una copia del database, possono consultarlo, devono passare da un ente centrale (o più soggetti valutatori) per modificarne i dati



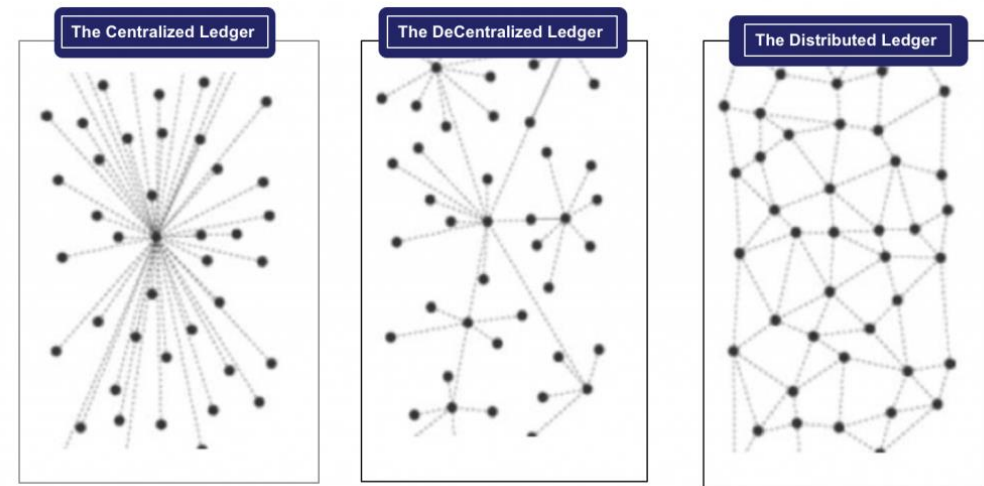
Distributed Ledger Technology

- ✓ La **Distributed Ledger technology (DLT)** è dunque un Sistema digitale che registra la transazione delle risorse in cui le **transazioni** e i loro dettagli sono registrati in posti multipli allo stesso tempo. A differenza dei database tradizionali, i **distributed ledgers** non hanno nessun sistema di store centrale o funzionalità amministrativa.



Distributed Ledger e Blockchain a confronto

- ✓ **Blockchain e Distributed Ledger** sono le tecnologie che abilitano **l'Internet of Value**, che si fonda su **5 ingredienti: rete, algoritmi, registro distribuito, trasferimenti ed asset**.
- ✓ Vi è ancora molta **confusione** sul significato dei termini **Blockchain** e **Distributed Ledger**. Le **tecnologie Blockchain** sono incluse nella più ampia famiglia delle tecnologie **Distributed Ledger** a cui aggiungono alcune funzionalità tipiche di altre tecnologie e soluzioni.



Distributed Ledger e Blockchain a confronto

- ✓ Se nei cosiddetti **Distributed Database**, tutti i nodi che possiedono una **copia** del database possono consultarlo, ma devono passare da un **ente centrale** (oppure più soggetti **validatori**) per modificarne i dati, nei sistemi di **Distributed Ledger** le modifiche al **registro** vengono regolate tramite algoritmi di **consenso**.
- ✓ Tali **algoritmi** permettono di raggiungere il **consenso** tra le varie versioni del **registro**, nonostante esse vengano aggiornate in maniera **indipendente** dai partecipanti della rete. Oltre agli algoritmi di **consenso**, per mantenere la **sicurezza** e l'**immutabilità** del registro, **Distributed Ledger** e **Blockchain** fanno anche un **ampio utilizzo della crittografia**.

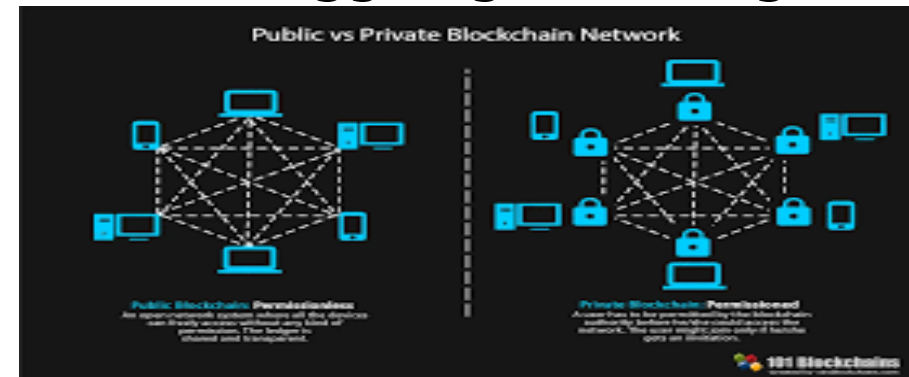


Caratteristiche delle Distributed Ledger Technology

- ✓ Proprio per la **particolarità** e la **rilevanza** della modalità con cui la rete aggiorna il registro, le caratteristiche fondamentali che distinguono i vari sistemi di **Distributed Ledger** sono tre:
 - tipologia di rete
 - meccanismo di consenso
 - struttura del registro
- ✓ Le **soluzioni** più propriamente dette **Blockchain**, quelle che si ispirano alla piattaforma **Bitcoin**, aggiungono due ulteriori caratteristiche che non necessariamente si trovano nei sistemi di **Distributed Ledger**: trasferimenti e asset.

Permission Ledger e Permissionless Ledger

- ✓ Sulla base della **tipologia di rete**, si distingue tra sistemi:
 - **permissioned** - reti in cui per accedere bisogna registrarsi e identificarsi e quindi essere autorizzati da un ente centrale o dalla rete stessa;
 - **permissionless** - reti in cui chiunque può accedere senza autorizzazione.
- ✓ **Nei sistemi permissioned il meccanismo di consenso è più semplice:** quando un nodo propone una l'aggiunta di una transazione, ne viene verificata la validità e si vota a **maggioranza** sull'opportunità di aggiungerla al registro.

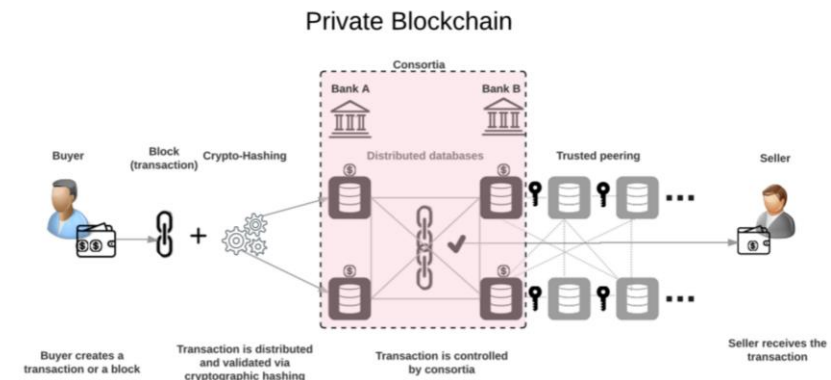


Permission Ledger e Permissionless Ledger

- ✓ In sistemi **permissionless**, invece, i meccanismi di consenso sono più complessi (basati ad esempio **Proof of Work** o **Proof of Stake1**) per evitare che un soggetto **malevolo** possa creare numerose identità **fittizie** e influenzare il processo di **modifica** del **registro**.
- ✓ Le **permissioned ledgers**, con permesso appunto, prevedono l'esistenza di uno o più attori **pre-selezionati** che svolgono la funzione di **validatore** nel network. Se il **validatore** è un solo agente viene definita come **DLT privato**, mentre se il **validatore** è più di uno viene definito come **DLT consortium**.

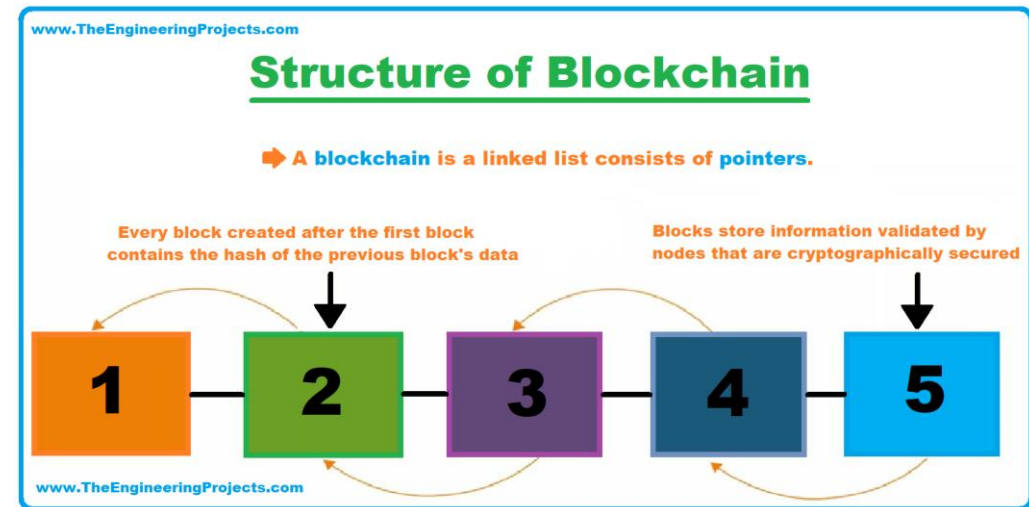
Permission Ledger e Permissionless Ledger

- ✓ Le **permissioned ledgers** permettono poi di definire speciali regole per **l'accesso** e la **visibilità** di tutti i dati.
- ✓ Introducono quindi nella **blockchain** un concetto di **governance** e di definizione di **regole di comportamento**.
- ✓ Le **permissioned ledgers** sono **più performanti, veloci e più vicine alle esigenze delle imprese** rispetto alle **permissionless Ledgers**.



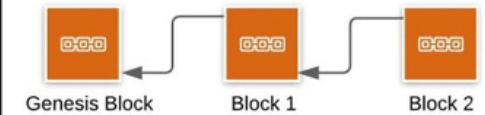
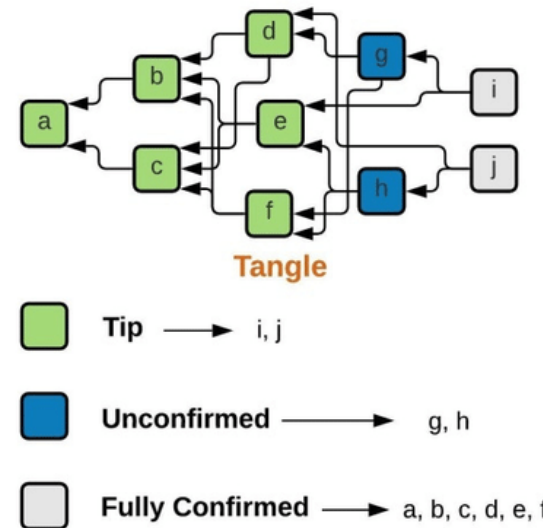
Caratteristiche dei Sistemi Blockchain

- ✓ Un'altra caratteristica dei sistemi **Distributed Ledger** è la struttura del registro. Le soluzioni **Blockchain** sono quelle in cui il registro è strutturato come una **catena** di blocchi contenenti più **transazioni** e i blocchi sono tra di loro **concatenati** tramite **crittografia** (come ad esempio nelle piattaforme **Bitcoin** o **Ethereum**).



Caratteristiche dei Sistemi Blockchain

- ✓ Vi sono poi soluzioni **Distributed Ledger** in cui il **registro** è formato da **Tangle**, dove cioè le transazioni vengono processate in **parallelo** (ad esempio **IOTA**) e non sequenzialmente come nella catena o altri casi ancora in cui il **registro** è formato da una **catena di transazioni** (ad esempio **Ripple**).

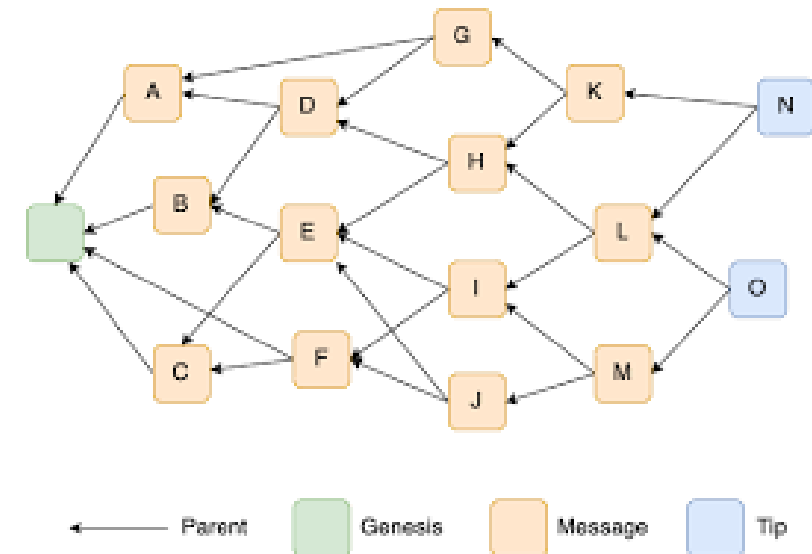


Blockchain

Cryptographically secured using timestamp, merkle tree, and the hash of the previous block is linked with the next block.

IOTA (criptovaluta)

- ✓ **IOTA** è un progetto **open-source**, che consiste in un **token crittografico**, di nuova generazione, già distribuito, quindi non minabile.
- ✓ È una **criptovaluta** focalizzata a fornire comunicazioni e forme di pagamento sicure tra le macchine nel contesto dell' **internet delle cose (internet of things)**. Il progetto organizza le informazioni sulle transazioni in una struttura detta «**tangle**», ossia un **grafo aciclico diretto**, diversamente dalla tradizionale **blockchain**.



IOTA (criptovaluta)

- ✓ Con il **tangle**, ogni transazione, per essere inserita in modo corretto, deve **validarne** altre due precedenti, non ancora validate. Questo elimina di fatto la differenza tra **utenti** e **minatori**, presente con la **blockchain**, perché la validazione non è basata sulla **competizione** tra **nodi**, ma viene eseguita in modo distribuito e uniforme da tutti i partecipanti della rete. Questo porta a 2 risultati particolarmente significativi:
- 1. **IOTA** è, in teoria, infinitamente **scalabile**, perché, all'aumentare del numero di transazioni, aumenta il numero di transazioni validate (ogni nuova transazione ne valida 2 precedenti). Nella blockchain invece, l'inserimento a velocità costante di un blocco alla blockchain, mediamente ogni 10 minuti, è di fatto un collo di bottiglia per le prestazioni della rete.

IOTA (criptovaluta)

2. non sono state introdotte **fee (commissioni)** per le **transazioni**, in quanto ogni nodo partecipa allo stesso **modo** alla **rete**, senza **competizione**, e dunque, per **mantenere** un **nodo**, non vi è la necessità di **investire** in **hardware sempre** più costosi (**come** invece avviene per il **mining** della **blockchain**). In tal modo è stata la prima **criptovaluta** senza costi di **transazione**, con la quale è possibile **trasferire** qualunque **importo senza commissioni**.
- ✓ **IOTA** è stata fondata nel **2015** da David Sønstebø, Sergey Ivancheglo, Dominik Schiener, e Dr. Serguei Popov. Nell'estate del 2016 è in fase **beta** di test. A dicembre **2017** la **capitalizzazione** di mercato di **IOTA** è stata di oltre **12 miliardi** di dollari statunitensi, rendendola la **4ª criptovaluta** al mondo **per capitalizzazione**.

IOTA (criptovaluta)

- ✓ A **differenza** dei circa **21.000.000** di **Bitcoin minati** e **minabili** complessivamente, ci sono **2.779.530.283.277.761 IOTA** in circolazione, già tutti **distribuiti**.
- ✓ Dato l'attuale cambio rispetto alle valute **fiat**, l'unità di misura ricorrente per riferirsi alla **criptovaluta** non è lo stesso **IOTA**, ma il **MIOTA**, ossia un **milione di Iota**.
- ✓ Il progetto **Iota** collabora attualmente con **Ubuntu/Canonical, Innogy, Microsoft, Cisco, Foxconn, Bosch** e altre aziende.
- ✓ La **IOTA** Foundation sta sviluppando modelli di **microtransazioni** per il mercato delle telecomunicazioni, con **Microsoft** collabora alla piattaforma Azure e con Cisco, Foxconn e Bosch ha cofondato la **Trusted** IoT Alliance.

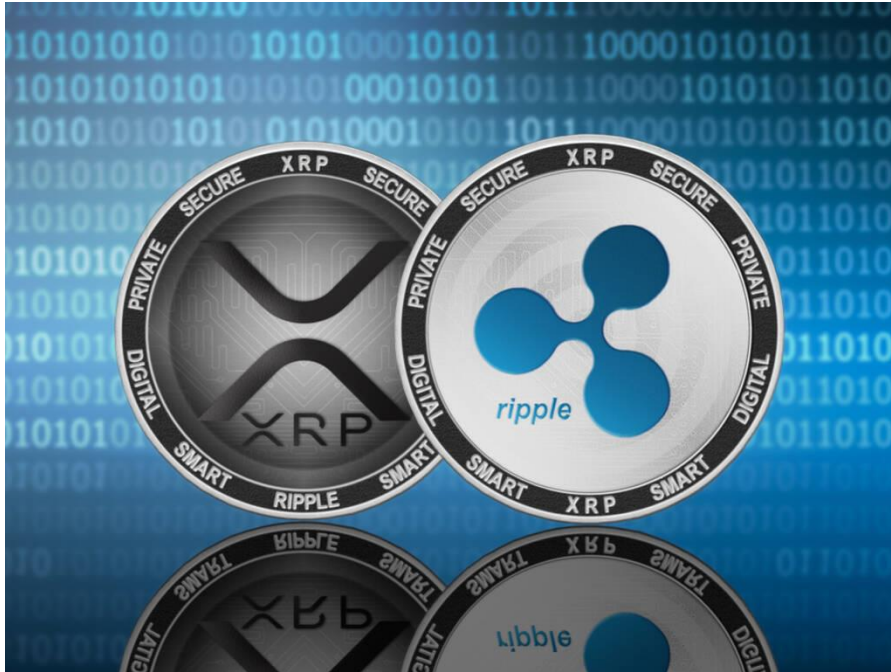
IOTA (criptovaluta)

- ✓ Generalmente il concetto stesso di **criptovaluta** implica la **decentralizzazione** della stessa.
- ✓ Tuttavia dietro molte **coin** fra cui le principali **Bitcoin**, **Ethereum** e **Litecoin** ci sono pool di utenti definiti "**miner**" che hanno il compito di **minare** nuove unità e approvare transazioni delle rispettive **criptovalute**.
- ✓ Ciò comporta, in **contraddizione** al principio di valuta **elettronica** una **centralizzazione** del controllo delle **valute**.
- ✓ Con il progetto **IOTA** si ovvia a questi problemi, difatti viene meno la figura del **miner**, in quanto tutte le unità sono state rilasciate nella fornitura **iniziale**.
- ✓ Inoltre **IOTA** è davvero una moneta **decentralizzata**, infatti per effettuare ogni transazione, è necessario convalidarne altre due attraverso il software con cui si accede al proprio **wallet privato**.

IOTA (criptovaluta)

- ✓ Quindi **tecnicamente** tutti gli utenti sono essi stessi **miner** che effettuano operazioni simili al **mining** ogni volta che richiedono **nuove transazioni**. Ne consegue che **IOTA** non ha **costi di commissione** nelle transazioni.
- ✓ La più piccola unità della valuta **IOTA** è lo **lota**. Tuttavia attualmente vengono utilizzati prevalentemente i suoi multipli indicati dai prefissi stabiliti dal sistema **metrico decimale** e seguiti dalla **parola lota**.
- ✓ Il multiplo attualmente più utilizzato (2017) è il **Megalota**.
- ✓ La Fondazione **IOTA** è stata registrata in **Germania** come una **società senza scopo di lucro** che coordina e finanzia gli sviluppi del **progetto IOTA**. A partire dal novembre **2017**, la **Fondazione** ha destinato **100 milioni** di dollari per promuoverne il progetto.

Ripple (criptovaluta)



- ✓ **Ripple** è un sistema di **trasferimento di fondi in tempo reale (Real-time gross settlement)**.
- ✓ Un **network** per gli **scambi in valute** e per invio di **rimesse**, creato nel **2012** da **Ripple Labs**, all'epoca **OpenCoin**.
- ✓ Il nome del **sistema**, per **esteso**, è **Ripple Transaction Protocol**, in sigla **RTXP** (traducibile in italiano come **Protocollo di transazione Ripple**, o semplicemente **Protocollo Ripple**).

Ripple (criptovaluta)

- ✓ Si basa su un **protocollo** Internet **Open Source**, in cui le **transazioni** sono **registrate** su un **libro mastro distribuito** (la cui integrità e affidabilità sono garantite da un sistema di verifica basato sul consenso, e su una propria **valuta digitale**, chiamata **XRP**).
- ✓ Lo scopo è di rendere possibili **transazioni finanziarie gratuite** e a livello **globale** di qualsiasi importo senza **chargeback** (contestazioni da parte dei titolari di una **carta di credito**).
- ✓ Il sistema si serve di "**token**" che rappresentano una **tradizionale valuta legale** (fiat currency), **criptovaluta**, **commodities** o qualsiasi altra **unità di valore**, come i chilometri percorsi nei **programmi frequent flyer** o i minuti di **telefonia mobile**.

Ripple (criptovaluta)

- ✓ **Ripple** è realizzato attorno ad una **base di dati pubblica e condivisa**, che usa un **processo consensuale** per la verifica dei pagamenti in un processo **distribuito**.
- ✓ La **rete** è **decentralizzata** e può operare senza l'azienda **Ripple**.
- ✓ Tra i "**validators**" ci sono **aziende, internet service providers**, e il **MIT**.
- ✓ Adottato da società come **Unicredit, UBS e Banco Santander**, **Ripple** sta iniziando a esser usato come **infrastruttura tecnologica** da banche e **reti di pagamento**.
- ✓ **American Banker** spiega che dal punto di vista delle banche, **libri mastri distribuiti** come il sistema di **Ripple** hanno maggiori vantaggi rispetto a **criptovalute** come **bitcoin**, tra cui prezzo e sicurezza.

Ripple (criptovaluta)

- ✓ **XRP** è la **valuta nativa** della rete **Ripple** ed esiste solamente in questi sistemi.
- ✓ XRP è divisibile sulla base di **6 posizioni decimali**: quindi, la più piccola unità divisionale, chiamata "**drop**" (**goccia**), vale **1 milionesimo** di **1 XRP** (in altri termini, **1 milione di drop** equivalente a **1 XRP**).
- ✓ Alla nascita furono creati **100 miliardi di XRP**, senza ulteriore creazione di **base valutaria**, come da regole del **protocollo**.
- ✓ Il **sistema** è stato **progettato** come un **asset "scarso"** che decrementa la sua **disponibilità**. Non dipende da **terze parti** per il **rimborso**, è l'unica valuta della rete **Ripple** che non comporta un **rischio** per la **controparte**, ed è l'unico **asset nativo digitale**.

Ripple (criptovaluta)

- ✓ **XRP** ha avuto un **valore inferiore** a **€1,00** fino al **21 dicembre 2017**, il 4 gennaio 2018 ha raggiunto il massimo storico di **€3,23**. Il valore al 30 marzo 2023 è €0,50.
- ✓ Le altre valute della rete **Ripple** sono strumenti di **debito**.
- ✓ Agli utenti della rete **Ripple** non è richiesto di usare **XRP** come mezzo di scambio e di **accantonamento** del valore.
- ✓ A ogni profilo **Ripple**, tuttavia, è richiesto di aver una **piccola "riserva"** di **10 XRP**^[17] (**€5,00** al 30 marzo 2023).
- ✓ Lo scopo di questa **richiesta** è discussa nella sezione **anti-spam** del protocollo **Ripple**.

Ripple (criptovaluta)

- ✓ Fin dal suo debutto, il protocollo **Ripple** ha avuto l'attenzione sia della stampa finanziaria che di quella tradizionale di massa.
- ✓ **Ripple** è stato citato negli articoli settoriali da The Nielsen Company, **Bank of England Quarterly Bulletin**, NACHA e KPMG, con molti articoli che esaminano l'impatto di **Ripple** sull'internazionalizzazione del settore bancario.
- ✓ Nell'aprile 2015, **American Banker** sosteneva che «da un punto di vista bancario, i registri distribuiti come il sistema Ripple presentano diversi vantaggi rispetto alle **criptovalute** come il bitcoin», inclusa la sicurezza.
- ✓ Come ha scritto la **Federal Reserve Bank di Boston**, «l'adozione di reti distribuite come **Ripple** potrebbe aiutare il settore bancario a realizzare elaborazioni più rapide e a migliorare l'efficienza dei pagamenti globali e dei servizi bancari di corrispondenza».

Ripple (criptovaluta)

- ✓ Nel **2013** Ken Kurson ha dichiarato a **Esquire**, a proposito di **Ripple** come rete di pagamento, che «i grandi marchi di servizi finanziari dovrebbero trattare Ripple come le case discografiche hanno trattato **Napster**».
- ✓ Nell'agosto **2015**, **Ripple** ha ricevuto il premio come pioniere tecnologico (Technology Pioneer) dal World Economic Forum.
- ✓ Il sito **Dealbook** che appartiene a New York Times ha osservato nel 2014 che «(Ripple) sta catturando ciò che si è rivelato difficilmente raggiungibile per le valute virtuali: la partecipazione dei giocatori di **mainstream** al sistema finanziario»



Come funziona Ripple

- ✓ Il libro mastro distribuito di **XRP** (al contrario della tecnologia blockchain) supporta il trasferimento di token che rappresentano la fiat currency (moneta legale), criptovalute o qualsiasi altra unità di valore.
- ✓ Per **moneta legale** (o **moneta a corso legale**, **moneta fiduciaria** o, ancora, **moneta fiat**) si intende uno **strumento di pagamento** non coperto da riserve di altri materiali (ad esempio: riserve auree), e quindi privo di **valore intrinseco** (anche indiretto).
- ✓ Dal momento che il protocollo Ripple è completamente aperto, chiunque può accedervi senza approvazione a priori da parte dei **Ripple Lab**.
- ✓ Questo permette alle banche e attori non bancari di incorporare il protocollo Ripple nei propri **sistemi**.

Validazione della Transazione XRP

- ✓ Il libro mastro distribuito viene mantenuto da vari partecipanti indipendenti della comunità globale di **XRP**. Ogni transazione XRP richiede un agreement da parte dei nodi validatori. Questo agreement viene chiamato **consenso** e serve come insediamento finale e **irreversibile**.
- ✓ Il libro maestro raggiunge il **consenso** su tutte le transazioni ogni 3 o 5 secondi (mediando appena sotto i 4 secondi), al quale punto un nuovo libro viene rilasciato.
- ✓ Chiunque abbia la capacità di diventare un **validatore**, sul ledger oggi giorno può essere un università, istituzioni di scambio e persino finanziarie.
- ✓ Esistono **36 validatori**, con i Ripple Lab che lavorano su **6** nodi (tenendo in conto il **16%** della rete).

Caratteristiche di XRP

- ✓ **XRP** trae il suo valore da vari fattori, ma soprattutto dalla capacità di Ripple di lavorare con istituzioni e dalla abilità di essere scambiata in modo **rapido** ed **efficiente** per qualsiasi valuta o asset.
- ✓ **XRP** al momento ha 45404 miliardi di token in circolazione, mentre in totale può fornire circa 100 miliardi di token XRP.
- ✓ **Ripple Labs** ha inizialmente posseduto 55 miliardi di token XRP, con l'abilità di venderne 1 miliardo al mese,

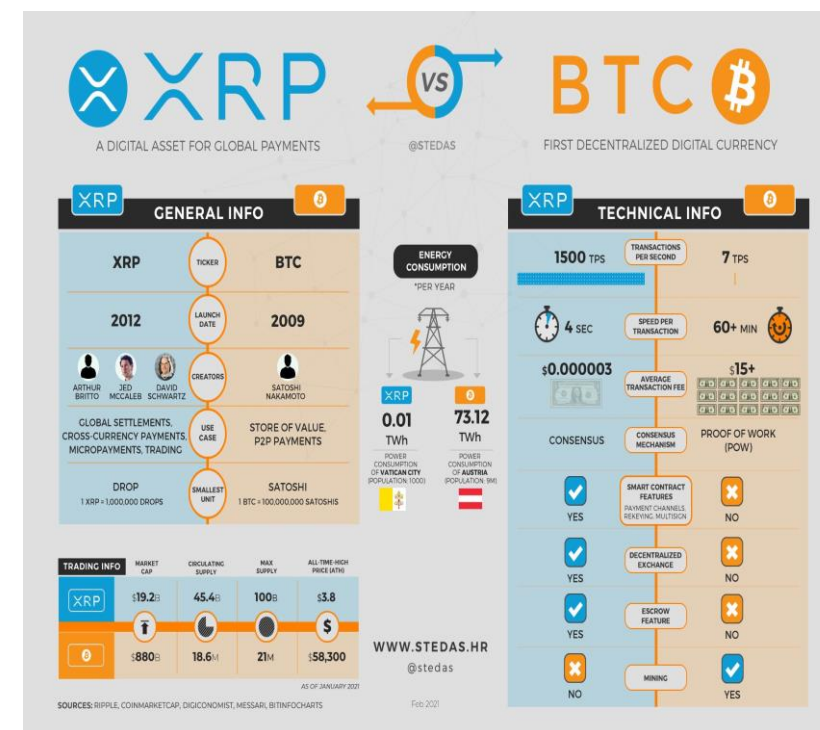


Come viene messa in sicurezza la rete Ripple?

- ✓ La differenza principale tra **XRP** e **Bitcoin** potrebbe essere riassunta nella differenza tra una company e una economia.
- ✓ La fornitura di **Bitcoin** trae il suo valore da vari fattori, ma soprattutto dalla capacità di Ripple di lavorare con istituzioni e dalla abilità di essere scambiata in modo **rapido** ed **efficiente** per qualsiasi valuta o asset.
- ✓ **XRP** al momento ha 45404 miliardi di token in circolazione, mentre in totale può fornire circa 100 miliardi di token XRP.
- ✓ La differenza tra **XRP** e **Bitcoin** potrebbe essere riassunta come la differenza tra company e economia.
- ✓ La fornitura di **Bitcoin** è rilasciata attraverso il processo di **mining** ad un tasso predeterminato dall'algoritmo matematico.

Come viene messa in sicurezza la rete Ripple?

- ✓ Le transazioni vengono processate nei Bitcoin in **un'industria di mining** decentralizzata.
- ✓ Dall'altro lato la fornitura di **XRP** viene rilasciata da una compagnia ad un tasso predeterminato da suoi dirigenti aziendali, mentre le sue transazioni vengono processate da un comitato di stakeholder pre-approvati.
- ✓ Questo la rende l'opzione perfetta per quelli che cosa non va con i meccanismi tradizionali bancari, ma non sono tanto confidenti nella decentralizzazione complete e senza controllo.



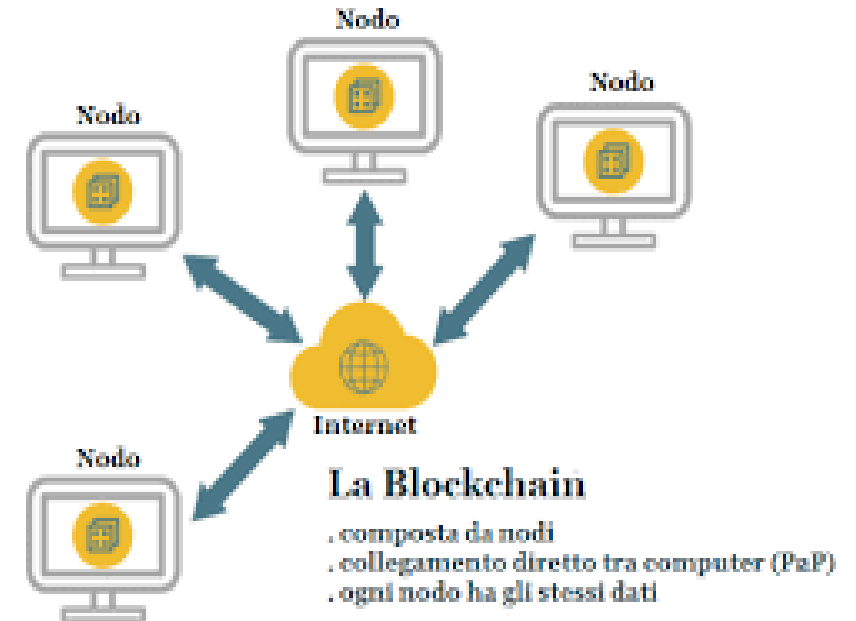
Blockchain



- ✓ Le tecnologie **Blockchain** sono dunque incluse nella più ampia famiglia delle tecnologie di **Distributed Ledger**, ossia sistemi che si basano su un **registro distribuito**, che può essere letto e modificato da più nodi di una rete.
- ✓ Per validare le modifiche da effettuare al registro, in assenza di un ente centrale, i nodi devono raggiungere il consenso. Le **modalità** con cui si raggiunge il **consenso** e la **struttura del registro** sono alcune delle caratteristiche che connotano le diverse tecnologie **Distributed Ledger**.

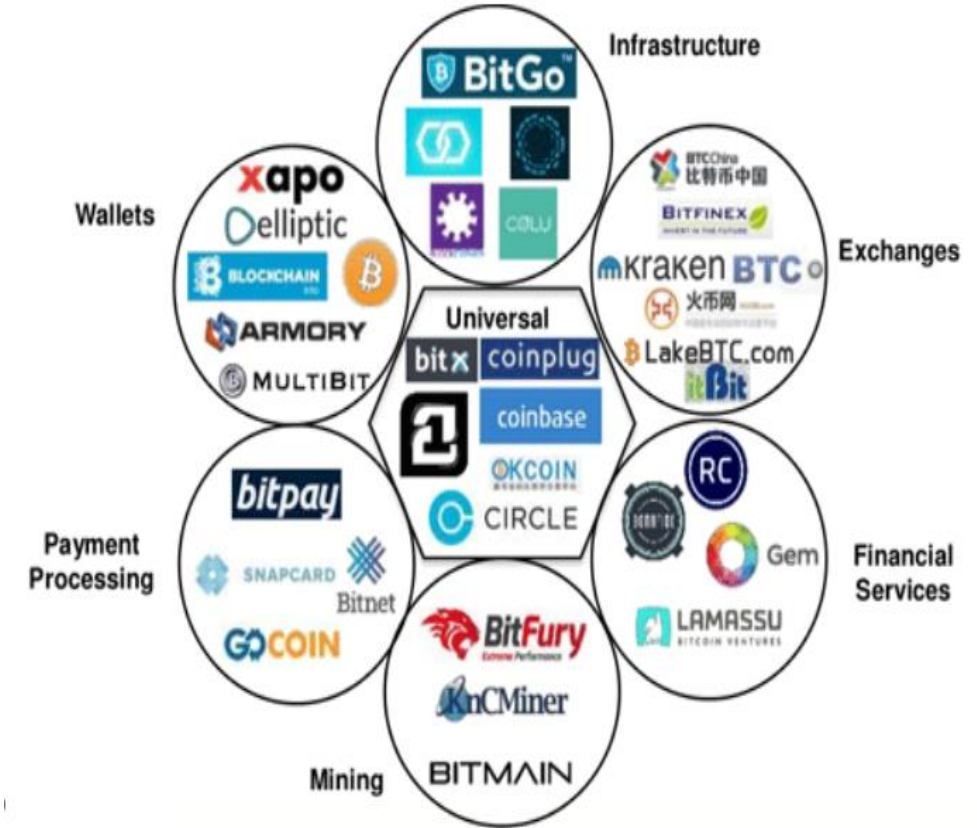
Blockchain

- ✓ La **Blockchain** è quindi una sottofamiglia di tecnologie, o come viene spesso precisato, un insieme di tecnologie, in cui il registro è **strutturato** come una **catena di blocchi** contenenti le transazioni e il consenso è distribuito su tutti i nodi della rete.
- ✓ Tutti i nodi possono partecipare al processo di validazione delle transazioni da includere nel registro.



Architetture di Blockchain

- ✓ **Un'Architettura Blockchain**, in sostanza, '**custodisce**' un deposito di dati formalmente costituito da una lista di record che continua a crescere, ma che resiste ad eventuali modifiche.
- ✓ Tutto inizia nel **2008**, anno che tutti ricordiamo per il **tracollo del sistema finanziario globale** di cui ancora oggi sentiamo le conseguenze.



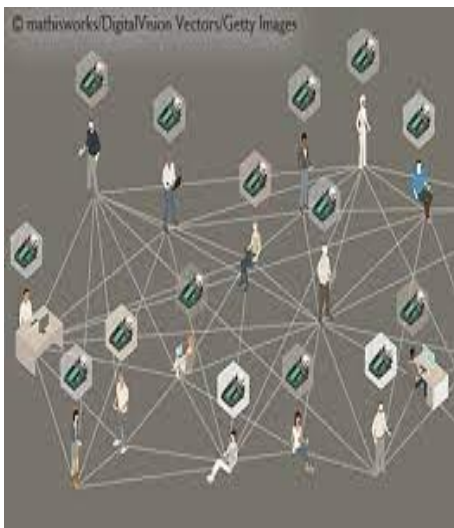
Architetture di Blockchain

- ✓ U Satoshi Nakamoto, personaggio attorno al quale tutt'oggi aleggia una **nube di mistero** pubblica il protocollo **Bitcoin** attraverso un white paper nel quale viene descritta **un'architettura tecnologica** atta a reggere la circolazione di bitcoin, **criptovaluta**, ossia moneta digitale la cui implementazione si basa sui principi della **crittografia** per convalidare le transazioni e la generazione di moneta stessa
- ✓ La moneta transita **liberamente** tra gli utenti senza costi sulle operazioni e senza il controllo di un organo centrale. **Bitcoin** con la maiuscola indica **l'architettura tecnologica** di cui sono stati rilasciati dettagli e codice nel **2009**, **bitcoin** con la minuscola indica la **moneta digitale criptata** la cui prima emissione risale al **2010**.

Architetture di Blockchain

- ✓ **L'architettura** che **'regge'** la fiducia distribuita è la **Blockchain**. La grande rivoluzione, da un punto di vista teorico, sta proprio **nell'assenza** di **'intermediari'**, come una **banca**; il libro contabile, il cosiddetto bank ledger, ossia il **libro mastro** sul quale viene registrata tutta la **contabilità di una banca**.

- ✓ Questo **libro mastro** ora diventa in realtà un **'distributed ledger'** accessibile da qualsiasi utente che effettui una transazione ed entri quindi a far parte della **'catena di distribuzione'**, cui è affidato il controllo dell'intero sistema o di una parte di esso (tutte le informazioni del **'libro mastro'** sono distribuite e condivise da tutti i soggetti del network, cioè da coloro che partecipano alla Blockchain).



Architetture di Blockchain



- ✓ Sebbene **Nakamoto** abbia dato il via **all'architettura Bitcoin** (cioè l'infrastruttura che sottende alla circolazione della moneta criptata bitcoin), in poco tempo il **concetto di Blockchain** ha preso il sopravvento.
- ✓ E' stato dunque identificata la **Blockchain** con **Bitcoin**, identificando appunto con esso il nome dell'infrastruttura e preferendo parlare di Blockchain e non di **Bitcoin** per evitare che venga culturalmente associata solo alla moneta bitcoin.

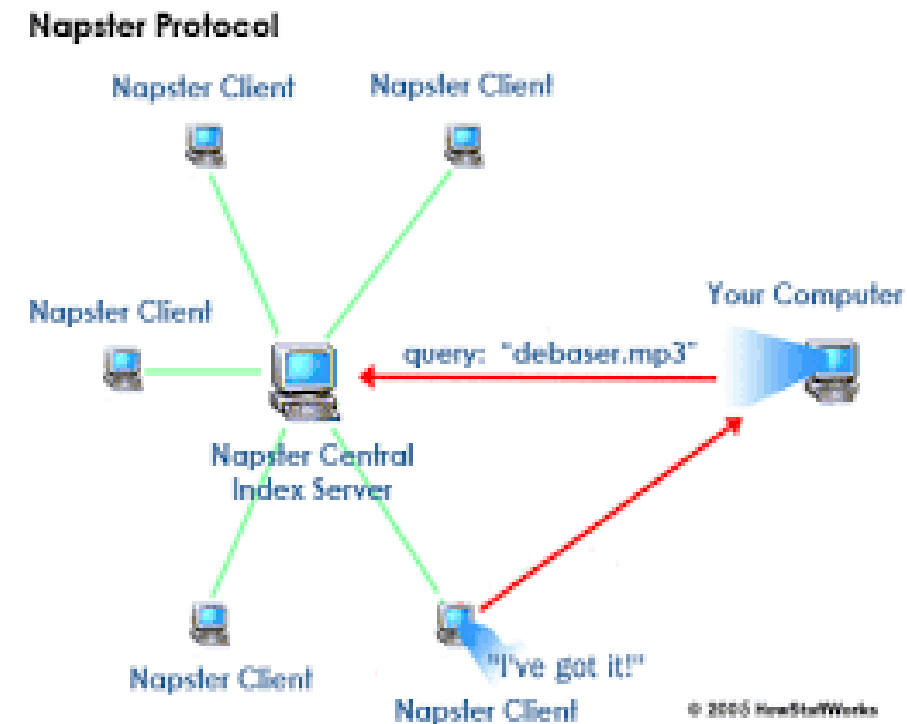
Architetture di Blockchain

- ✓ **Blockchain**, è più o meno dal 2013 che lo si utilizza per descrivere la piattaforma tecnologica che sta alla base di meccanismi di **'trust'** che potrebbero **abilitare** nuove forme di scambio (di **valuta**, di **beni**, di **informazioni**, di **contratti**, ecc.) dove la **fiducia** non è più riposta in una entità **centrale** ma **distribuita** tra tutti i partecipanti dello **'scambio'**.
- ✓ **Differenza** tra **Bitcoin** e **Blockchain**: **Bitcoin** è una **criptovaluta** mentre la **Blockchain** è un **database distribuito**, possiamo dire. Bitcoin ha trovato molti utilizzi aldilà della criptovaluta. Bitcoin promuove **l'anonymity**, mentre blockchain è per la trasparenza.



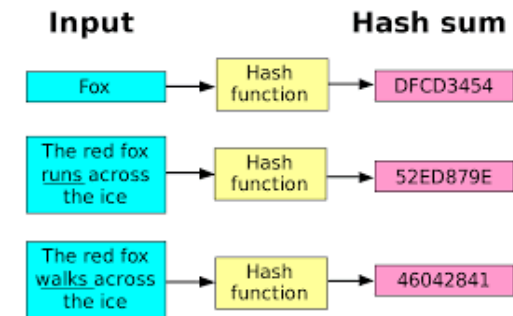
Architetture di Blockchain

- ✓ Le **tecnologie** alla base del funzionamento della **Blockchain** non rappresentano in realtà nulla di nuovo per il mondo **IT**.
- ✓ Si tratta di un **mix** di **soluzioni informatiche** che vanno dal **file sharing peer-to-peer** (tipo Napster) alla **crittografia**, in particolare a **chiave pubblica e privata** (algoritmi **asimmetrici** o **simmetrici** che si basano sull'utilizzo di chiavi per cifrare e decifrare una informazione) e la **crittografia hash**



Architetture di Blockchain

- ✓ La **crittografia hash** è un algoritmo matematico che **trasforma** dei dati di **lunghezza arbitraria** (per esempio un messaggio) in una stringa binaria di **dimensione fissa** chiamata '**valore di hash**'.
- ✓ Gli algoritmi di **questo tipo** sono **unidirezionali** quindi difficili da invertire, motivo per cui sono utilizzati nelle **firme digitali**, per **l'autenticazione** dei messaggi oppure proteggere le **credenziali private** degli utenti nell'accesso ai servizi digitali. Ciò che appare **rivoluzionario**, seppur con l'impiego di tecnologie già esistenti, è la loro **unione** nel formare quella che appunto viene riconosciuta come una '**catena di blocchi**'.



Architetture di Blockchain

- ✓ **Un'architettura Blockchain**, in sostanza, **'custodisce'** un deposito di dati formalmente **costituito** da una lista di record che continua a crescere, ma che **resiste** ad eventuali **modifiche**.
- ✓ Tale **deposito di dati** (il **distributed ledger** che nel mondo finanziario potrebbe essere **'paragonato'** al **libro contabile** della banca) risiede su ogni singolo nodo (computer) e non è quindi governabile e manipolabile da un ente centrale.



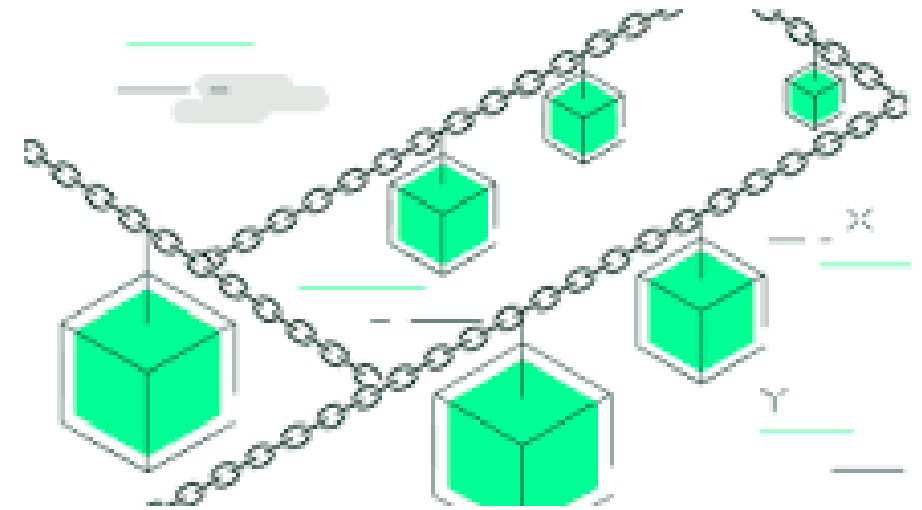
Architetture di Blockchain

- ✓ La **lista di record** contiene differenti tipi di **informazioni**: le **transazioni** (che contengono i dati di un fatto o un'operazione) e le **tracce** di come le transazioni vengono inserite nel **database distribuito** (che rappresentano i veri e propri blocchi).
- ✓ È importante comprendere la **differenza tra transazioni** e blocchi perché è su di essa che si basa anche la diversità tra utenti/partecipanti alla **Blockchain** e i cosiddetti '**miners**'.



Architetture di Blockchain

- ✓ I primi sono gli **utenti** che vogliono effettuare una **transazione** (per esempio trasferire un bene ad un altro).
- ✓ I secondi sono coloro che **creano i blocchi** e che inseriscono la transazione nel **database centralizzato** (generalmente a fronte di una '**ricompensa**' per il controllo effettuato sulla transazione, per non alimentare comportamenti illeciti che farebbero quindi cadere il meccanismo di fiducia della comunità).



Architetture di Blockchain

- ✓ I **Blocchi** sono i contenitori di base dell'informazione all'interno di una Blockchain.
- ✓ Contengono solo dati della transazione. Una volta aggiunti alla **Blockchain**, i blocchi non possono essere cambiati. I blocchi sono messi in sicurezza attraverso le tecniche **crittografiche**.
- ✓ Una **Blockchain** è esattamente ciò che suggerisce il **termine**: una catena costituita di blocchi di informazione. Questi blocchi sono contenitori che mantengono al loro interno un registro delle transazioni della blockchain. Nel caso del **Bitcoin**, le **transazioni** sono principalmente trasferimenti di bitcoin. Su alcune blockchain, esse possono anche contenere una certa varietà di altre informazioni, persino codice di **programmi al computer**.

Architetture di Blockchain

- ✓ In linea teorica, un **meccanismo** di **fiducia distribuita** a livello globale, sorretto da tecnologie **'nelle mani di tutti'**, senza la possibilità che tale sistema possa essere corrotto, risulta a dir poco **dirompente**.
- ✓ È bene rimanere sul fronte della **'teoria'** perché, in realtà, seppur i rischi di finire come in un film di **fantascienza** intrappolati all'interno di un'anarchica prigione **cibernetica** siano remoti, i limiti oggettivi allo sviluppo di una tecnica liberatrice e **disintermediante**, applicata a qualsiasi contesto, sono tutt'altro che superabili.
- ✓ Rimanendo all'interno dei nostri confini, quelli **It**, il funzionamento della **Blockchain** mostra evidenti difficoltà in termini di **scalabilità**. Per poter verificare un nuovo blocco o aggiungere una transazione all'interno della catena serve **tempo**.

Architetture di Blockchain

- ✓ Partendo dall'analisi fatta su **Bitcoin**, gli analisti di **Forrester** stimano che il **50%** dell'intero network in realtà lavori per questo tipo di operazioni e per ogni singola verifica, servano in media **10 minuti** (cosa che porta ad avere, all'interno di **Bitcoin**, **7 tps** – transazioni al secondo).
- ✓ “Paragonando questi dati alla media di **2500 tps** generate all'interno del circuito **Visa** che può reggere fino a 40mila e più **tps**, risulta **ancora** difficile pensare ad una **Blockchain scalabile**”, ammette **Martha Bennett** di **Forrester**. Vero è che il mondo si è mosso, soprattutto sul fronte **It**, dallo sviluppo di software per inviare, ricevere e gestire il proprio conto **bitcoin** (**Exchange bitcoin**, Greenbits, posteBit, Blockchain.info, solo per citare alcuni nomi), fino a coloro che costruiscono le infrastrutture od offrono servizi di pagamento.

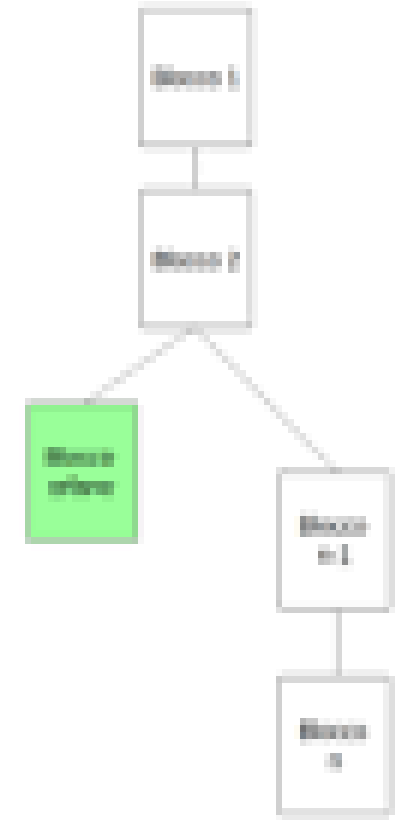
Architetture di Blockchain

- ✓ Dal **2010** ad oggi, attorno a algoritmi **Bitcoin/Blockchain** si è sviluppato un mercato di aziende **Ict** specializzate – che nel primo trimestre **2016** valeva già oltre **1 miliardo di dollari** – suddivise in **7 categorie**: **payment** processing, **infrastrutture**, **exchange**, **financial services**, **mining**, **wallet** e **'universal'** (quelle di carattere un po' più generale che lavorano magari in consorzi su specifici progetti di sperimentazione).



Architetture di Blockchain più nel dettaglio

- ✓ Una volta che le **transazioni** vengono aggiunte al **blocco**, esse non possono essere **rimosse**.
- ✓ E quando un **blocco** viene aggiunto alla **catena**, non può essere più cambiato. Tutte le **informazioni** che vengono mantenute nei blocchi vivranno lì finché la blockchain esiste.
- ✓ I **blocchi** vengono aggiunti sopra un altro in un modo sequenziale. Uno ad uno, questi blocchi formano una catena che contiene l'intera storia delle transazioni nella rete.
- ✓ L'esatta struttura dei blocchi differisce da una **blockchain** a **blockchain**, anche se c'è una base comune per tutti.



Architetture di Blockchain più nel dettaglio

- ✓ La **blockchain** (in italiano: blocchi concatenati) è una struttura dati che consiste in elenchi crescenti di **record**, denominati "**blocchi**", collegati tra loro in modo sicuro utilizzando la **crittografia**. Ogni blocco contiene un **hash crittografico** del blocco precedente, un **timestamp** e **dati di transazione**.
- ✓ Poiché **ogni blocco** contiene **informazioni** sul blocco **precedente**, questi **formano** effettivamente una **catena** con ogni blocco **aggiuntivo** che si collega a quelli precedenti. Di conseguenza, le transazioni **blockchain** sono **irreversibili** in quanto, una volta **registrate**, i dati in un determinato blocco non possono essere **modificati retroattivamente** senza alterare tutti i blocchi successivi.
- ✓ La **blockchain** rientra nella più ampia famiglia dei **registri distribuiti** (**distributed ledger**), ossia sistemi che si basano su un **registro replicato, condiviso e sincronizzato** tra più soggetti presenti in molteplici luoghi, ma comunque appartenenti alla **medesima entità**.

Architetture di Blockchain più nel dettaglio

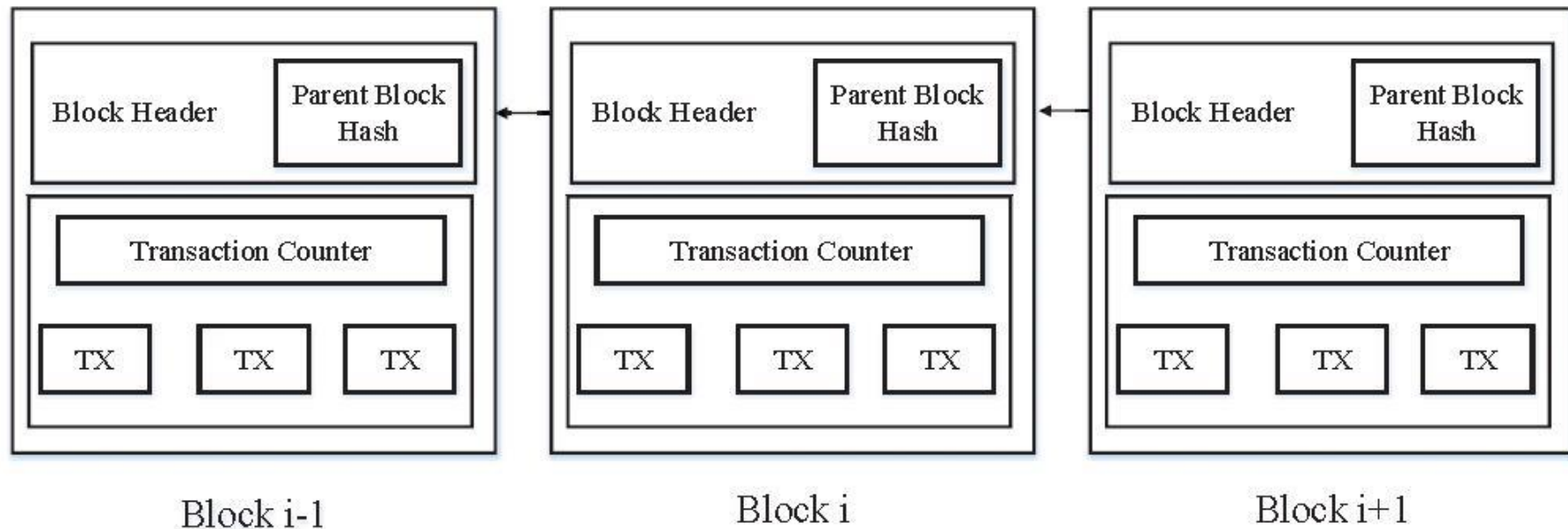
- ✓ Nel caso della **blockchain** non è richiesto che i **nodi** coinvolti conoscano l'identità **reciproca** o si fidino l'uno dell'altro perché, per garantire la **coerenza** tra le varie copie, l'aggiunta di un nuovo blocco è **globalmente regolata** da un **protocollo** condiviso.
- ✓ Una volta **autorizzata** l'aggiunta del **nuovo blocco**, ogni nodo aggiorna la propria **copia privata**. La natura stessa della **struttura** dati garantisce l'assenza di una sua **manipolazione** futura.
- ✓ Le **caratteristiche** che accomunano i sistemi sviluppati con le tecnologie della blockchain e dei registri distribuiti sono: **digitalizzazione** dei dati, **decentralizzazione**, **disintermediazione**, **tracciabilità** dei trasferimenti, **trasparenza/verificabilità**, **immutabilità** del registro e **programmabilità** dei trasferimenti.

Architetture di Blockchain più nel dettaglio

- ✓ Grazie a tali **caratteristiche**, la **blockchain** è considerata pertanto un'alternativa in termini di **sicurezza**, **affidabilità**, **trasparenza** e **costi** alle **banche dati** e ai registri gestiti in maniera **centralizzata** da autorità riconosciute e **regolamentate** (**pubbliche amministrazioni**, **banche**, **assicurazioni**, **intermediari** di pagamento, ecc.).
- ✓ Elementi essenziali della Blockchain:
 - I **blocchi** sono i **contenitori** di informazioni all'interno della **Blockchain**.
 - Essi **contengono** dati di **transazione**.
 - Una **volta** aggiunti alla **blockchain**, un **blocco** non può essere **cambiato**.
 - I **blocchi** sono messi al **sicuro** usando i metodi **crittografici**.

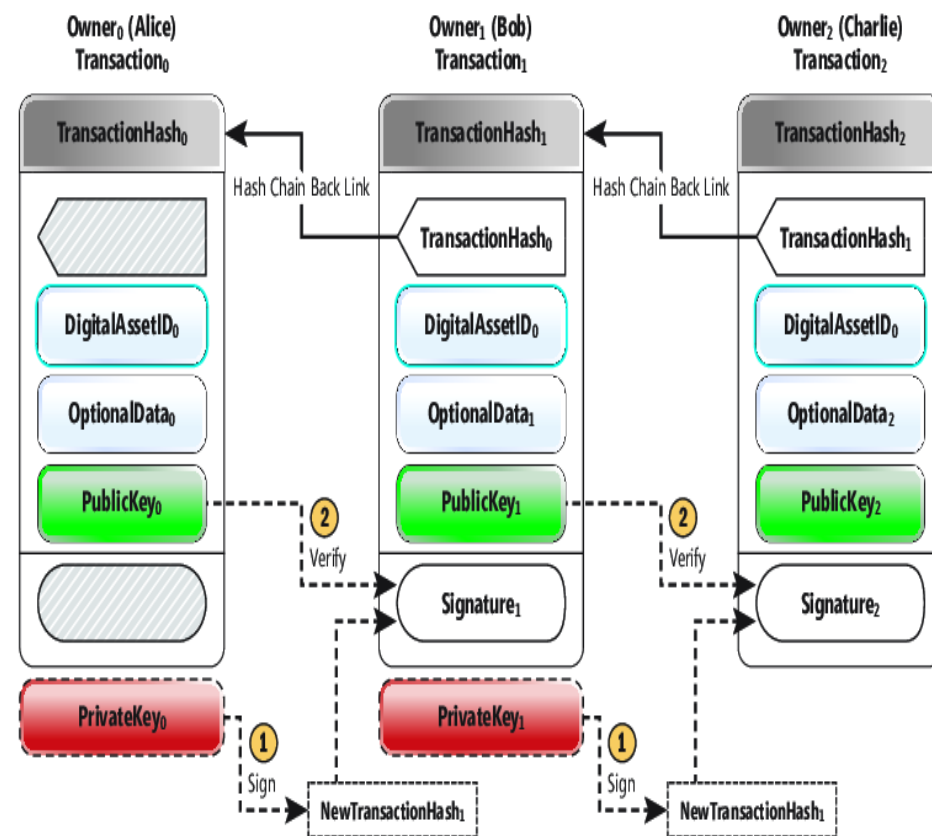
Le parti di un Blocco

- ✓ Il **corpo** di un **blocco** contiene i **record** di una **transazione**. **Immagazzinare** questi **record** con la massima **sicurezza** è una delle priorità della **blockchain**.
- ✓ Ma per essere in grado di funzionare in una **blockchain**, un blocco ha anche di bisogno di altri **4 elementi**. Ma prima di scoprire quali sono, vediamo prima come i dati vengono **memorizzati** all'interno di un **blocco**.



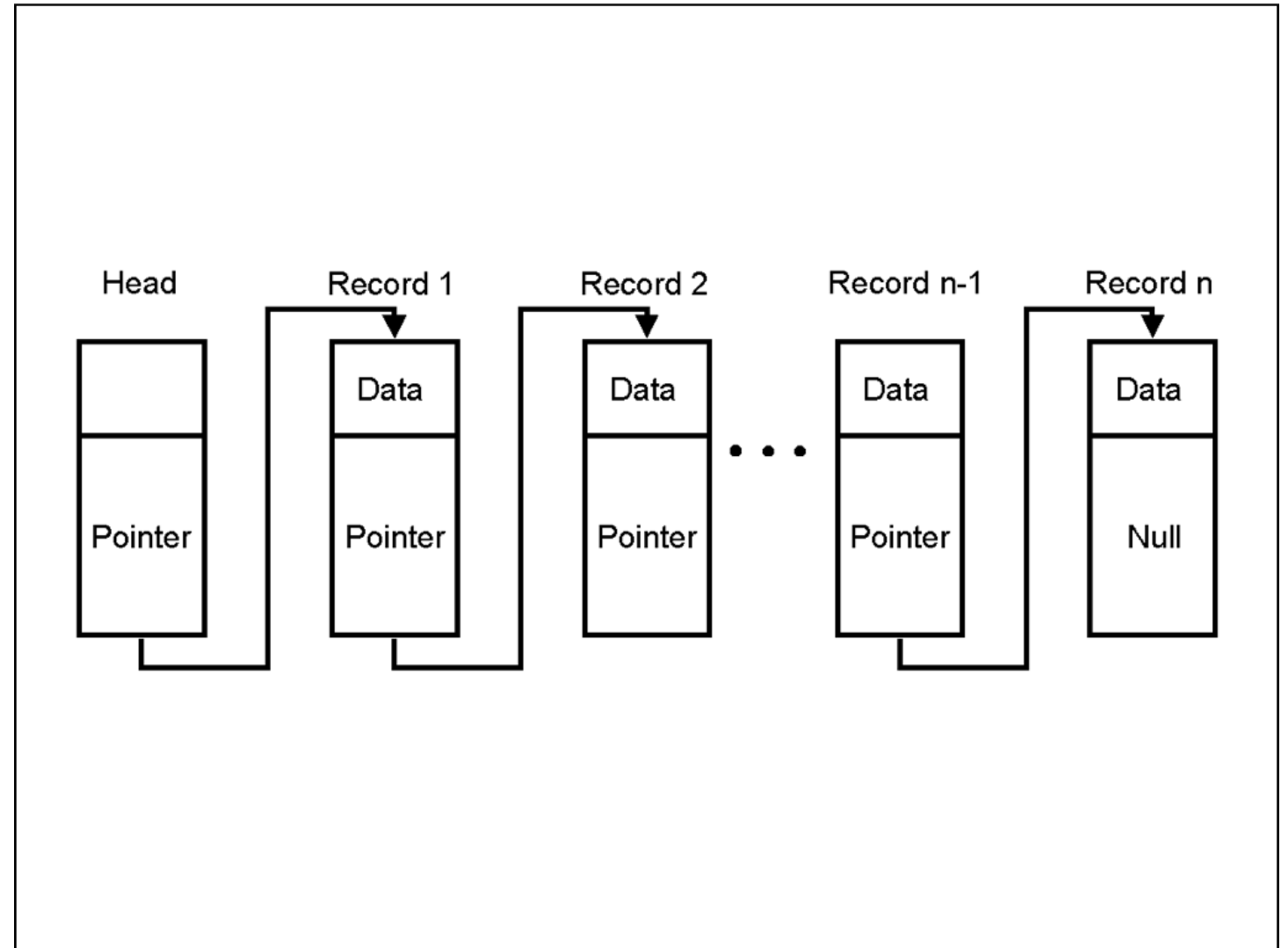
Le parti di un Blocco

- ✓ Le **Criptovalute** hanno guadagnato questo nome dal momento che si basano **pesantemente** sulla **crittografia**.
- ✓ Nel caso dei blocchi, la crittografia principalmente usata è chiamata **funzione hash**. Una stringa di simboli, chiamata **hash**, viene determinata attraverso un algoritmo di **hashing algorithm**.
- ✓ Il **Bitcoin** usa **SHA-256**, ma non tutte le **criptovalute** usano lo stesso algoritmo. Questo algoritmo prende tutti i dati presenti in un blocco e li **trasforma** in un'unica **stringa** di simboli che hanno la funzione di **ID** del **blocco**.



Le parti di un Blocco

- ✓ Nella **blockchain**, l'**hash** è una funzione **crittografica** che serve a condensare gruppi di transazioni in **blocchi**, **collegare ciascun blocco** con il successivo, e **identificare** ogni blocco.
- ✓ L'**hash** infatti è spesso usato per **identificare** e **trovare** una transazione sulla **blockchain**.



Le parti di un Blocco

- ✓ L'hash di un **blocco** (ossia l'**header** del blocco) è formato da **sei elementi** che costituiscono un blocco:
 - Il **numero** di **versione** del blocco,
 - L'**hash** del **precedente blocco** nella catena,
 - Un **codice** generato dai **dati** della transazione,
 - Un **timestamp** relativo a quando il **blocco** è stato creato,
 - L'ostacolo **dell'obiettivo** che aggiusta l'ostacolo del **mining**,
 - E una stringa casuale di caratteri chiamata "the nonce".
- ✓ Tutti, **eccetto** l'ultimo di questi elementi sono conosciuti in **anticipo** prima che un **blocco** sia **aggiunto** alla **catena**.

Bibliografia

https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni

<https://www.zerounoweb.it/cio-innovation/blockchain-architettura-applicazioni-scenari-futuri/>

<https://www.fortuneita.com/2021/12/10/la-nuova-strada-del-crypto-il-mining-a-rate/>

<https://www.bitstamp.net/learn/crypto-101/what-are-blocks-in-the-blockchain/>

<https://youngplatform.com/glossary/hash/>

https://blog.osservatori.net/it_it/distributed-ledger-technology-significato

Bibliografia

<https://www.informamuse.com/una-blockchain-due-tipi-di-ledger-permissionless-o-permissioned/>

[https://it.wikipedia.org/wiki/IOTA_\(criptovaluta\)](https://it.wikipedia.org/wiki/IOTA_(criptovaluta))

<https://kriptomat.io/cryptocurrencies/xrp/what-is-xrp/>