

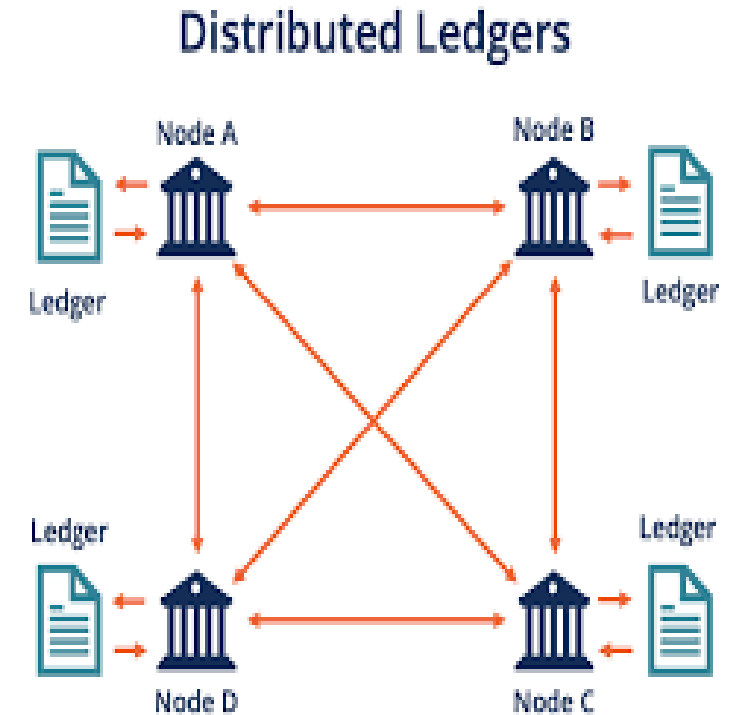
Distributed Ledger Technology

Francesco Pugliese, PhD

neural1977@gmail.com

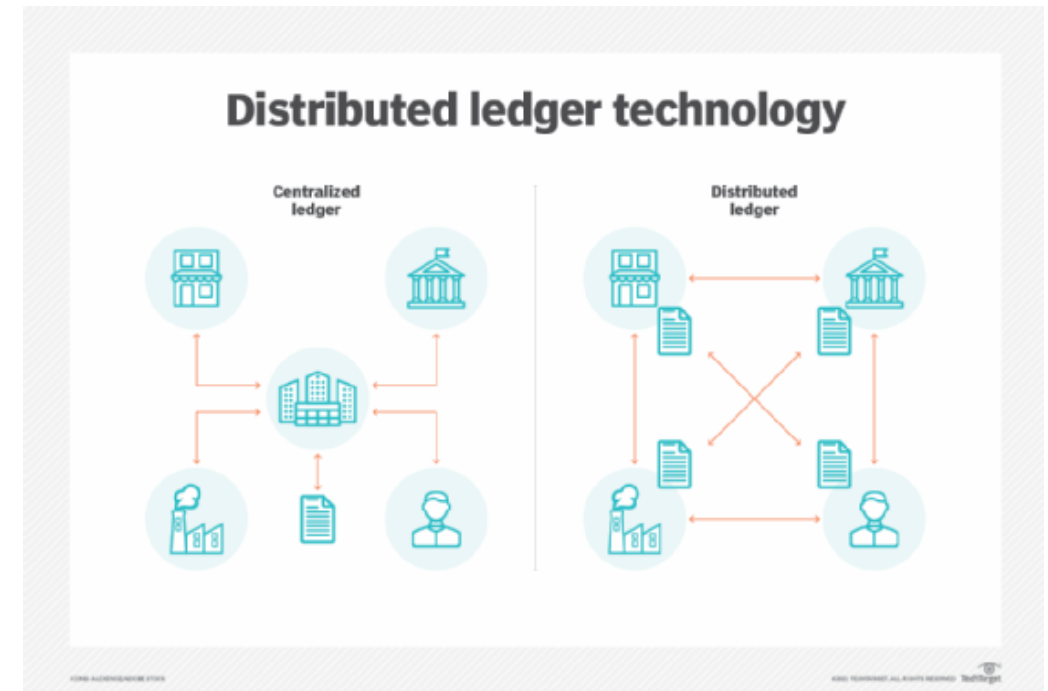
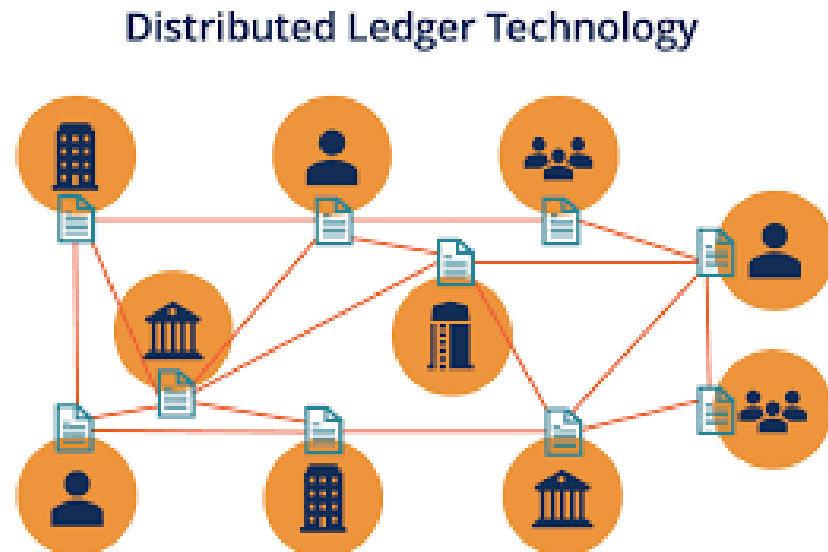
Distributed Ledger Technology

- ✓ 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.



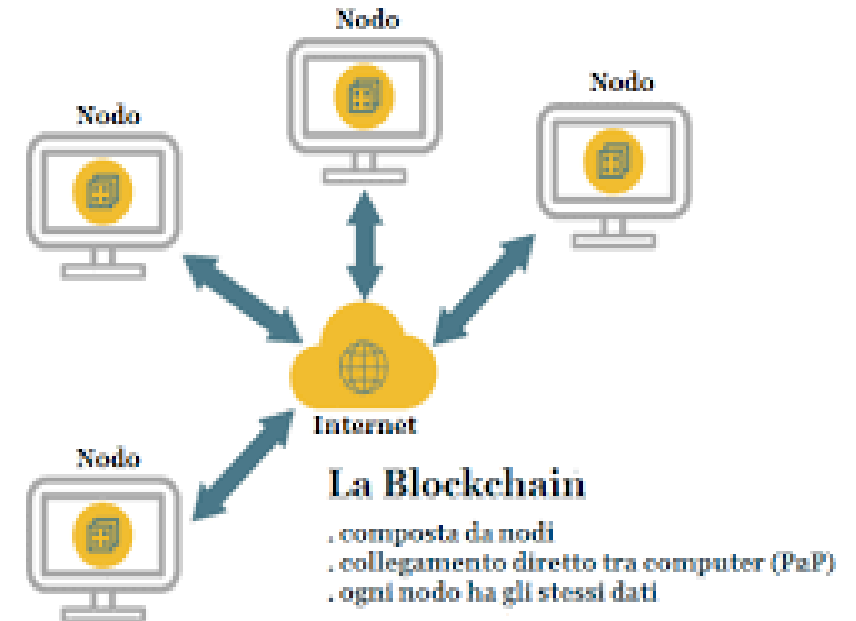
Blockchain



- ✓ 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**.

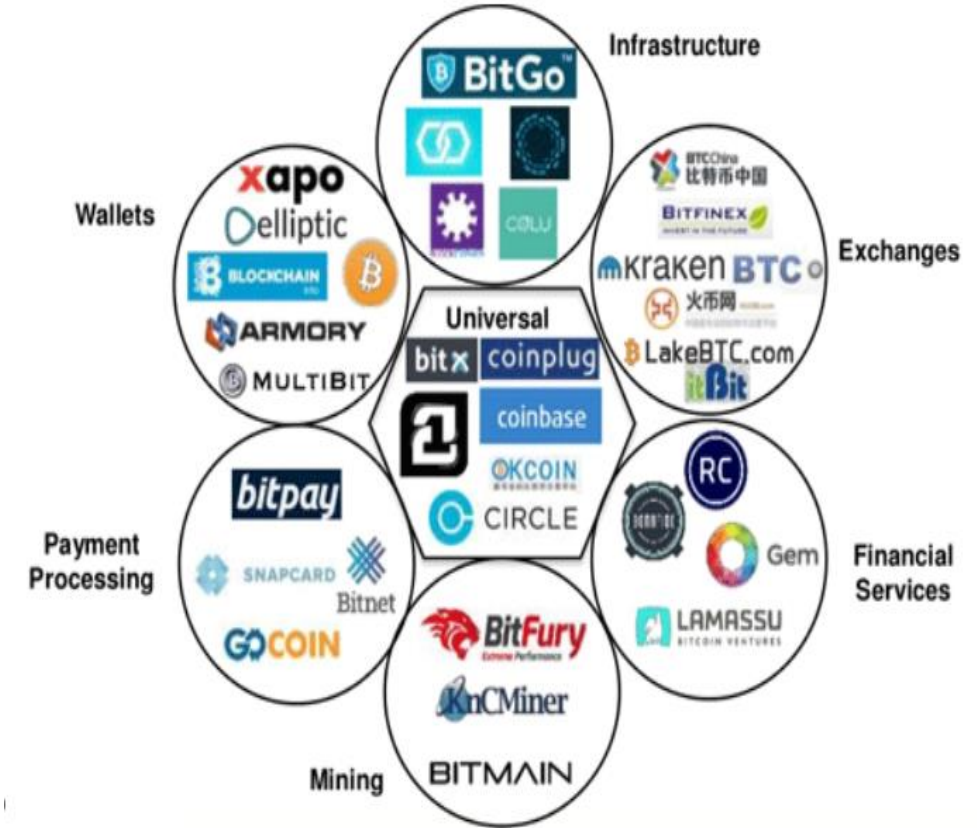
Blockchain

- ✓ 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.



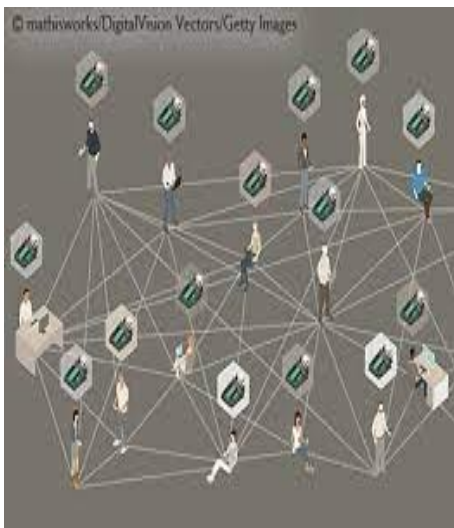
Architetture di Blockchain

- ✓ 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.

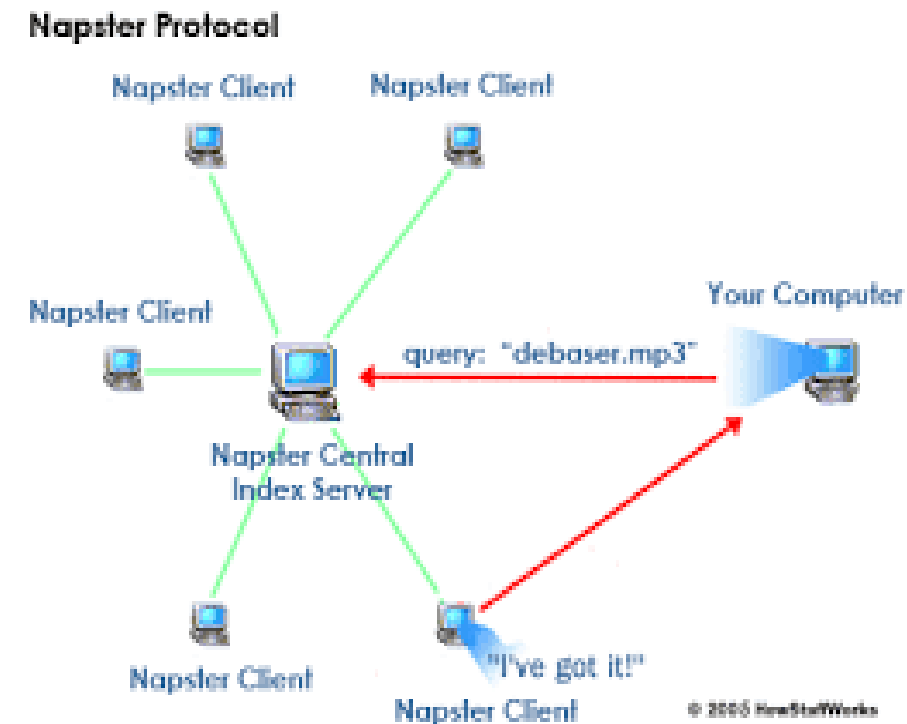
Architetture di Blockchain

- ✓ **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.



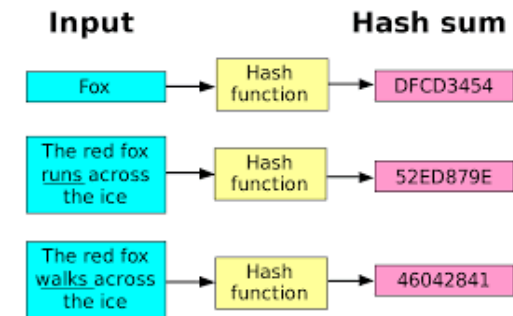
Architetture di Blockchain

- ✓ 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**'.



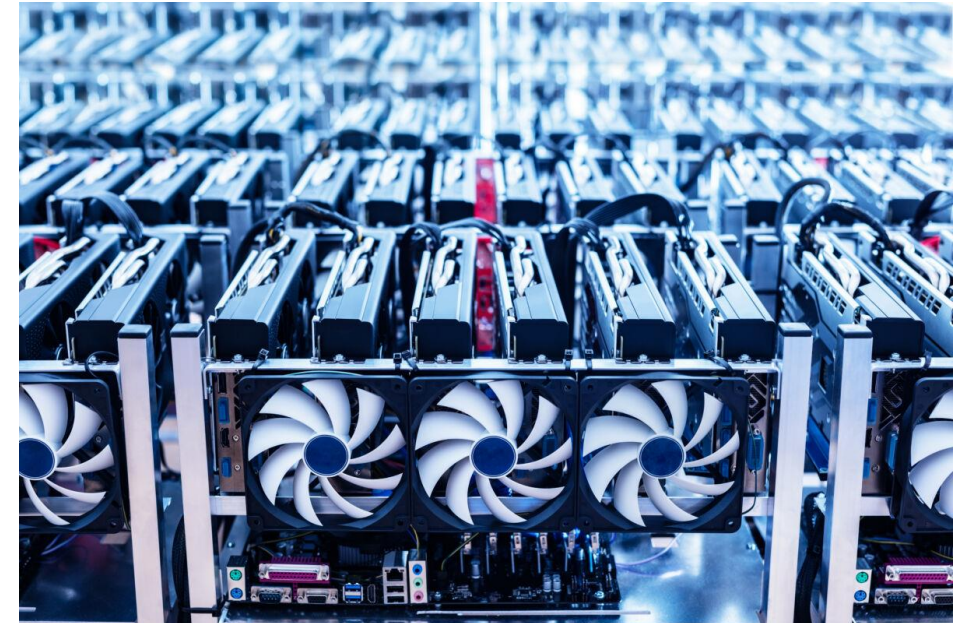
Architetture di Blockchain

- ✓ **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.



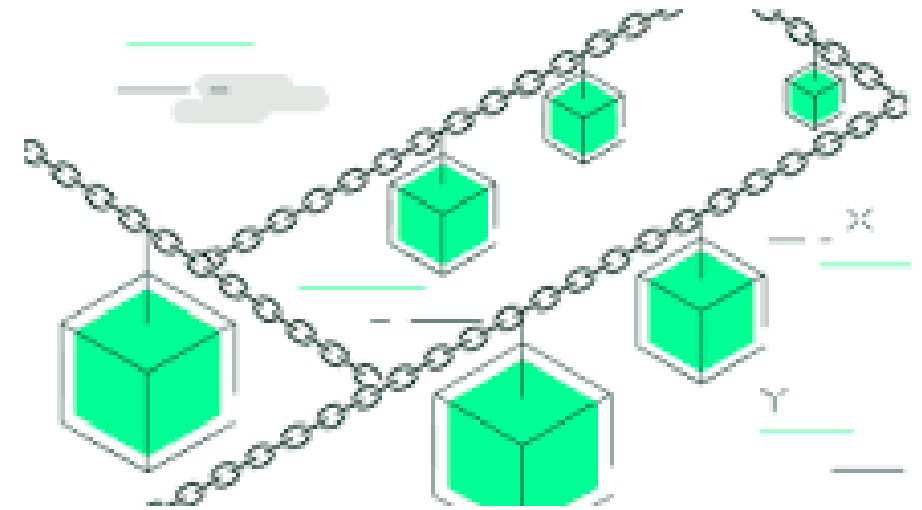
Architetture di Blockchain

- ✓ 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.

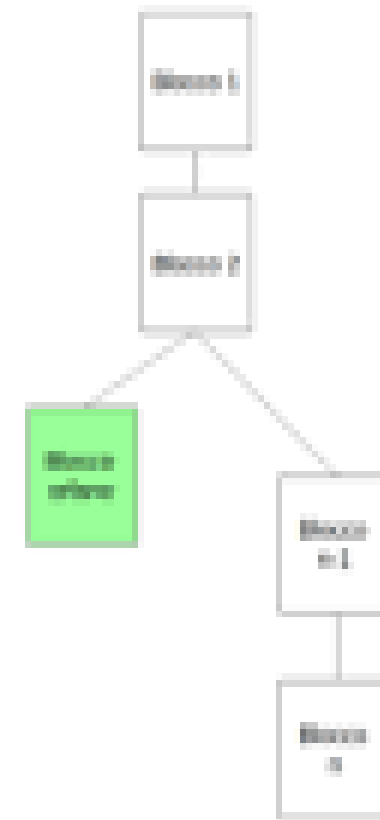
Architetture di Blockchain

- ✓ 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

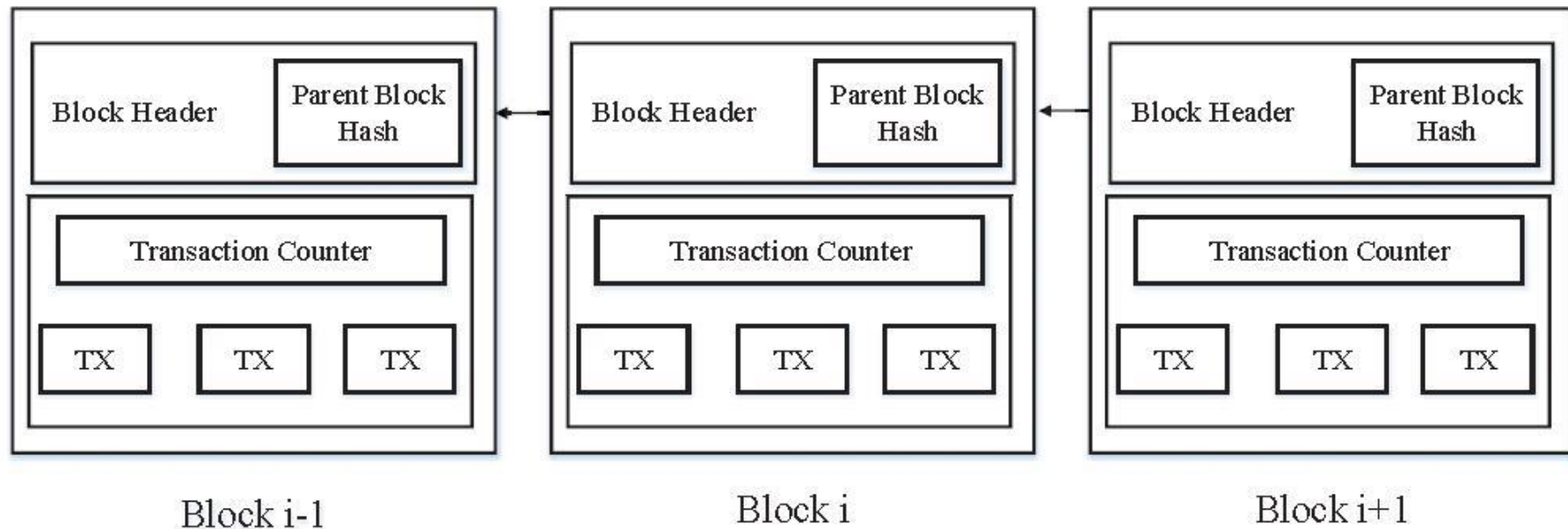
- ✓ Nel caso della **blockchain** non è richiesto che i **nodi** coinvolti conoscano l'identità **reciproca** o si fidino l'uno dell'altro perché, per garantire la **coerenza** tra le varie copie, l'aggiunta di un nuovo blocco è **globalmente regolata** da un **protocollo** condiviso.
- ✓ Una volta **autorizzata** 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**.

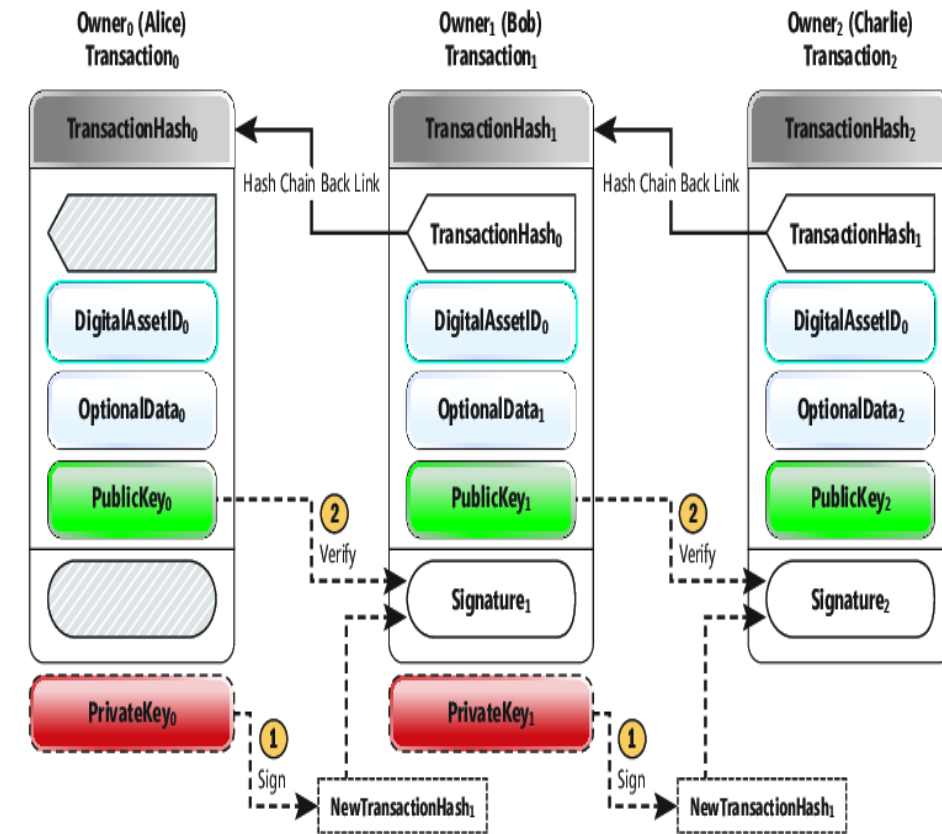
Le parti di un Blocco

- ✓ 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**.



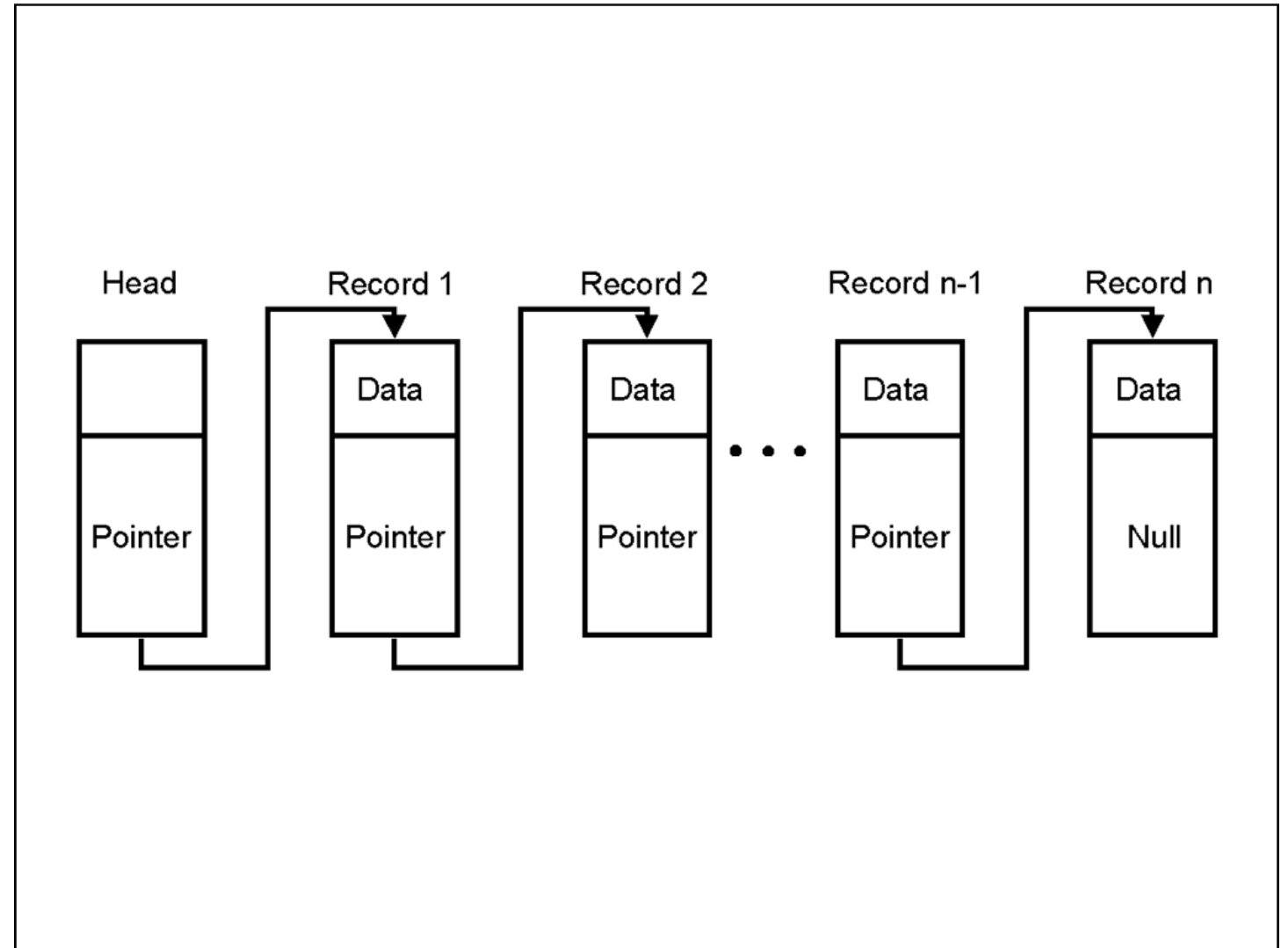
Le parti di un Blocco

- ✓ 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 determinate 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** relative a quando il **blocco** è stato creato,
 - L'ostacolo **dell'obiettivo** che aggiusta l'ostacolo del **mining**,
 - E una stringa casual 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/>