Fondamenti di Blockchain

Albenzio Cirillo
acirillo@fub.it

Corso Spettro Radio
14 giugno 2023

FUB
Fondazione Ugo Bordoni
Ricerca e Innovazione

Le origini della blockchain

Fra' Luca Pacioli
considerato il fondatore della moderna ragioneria e padre del registro a partita doppia

Satoshi Nakamoto, nel 2009, pubblica un paper intitolato «*Bitcoin: un sistema di moneta elettronica peer-to-peer*».
L'idea della blockchain nasce quindi dalla volontà di creare un sistema di pagamento elettronico basato su prova crittografica invece che sulla fiducia

- Senza la necessità di una Trusted Third Party
- Riducendo i costi di intermediazione

La blockchain è *disruptive* perché offre l'opportunità di rivoluzionare quei processi che finora hanno richiesto l'intervento di un soggetto terzo, avente il ruolo di parte fidata tra i partecipanti.

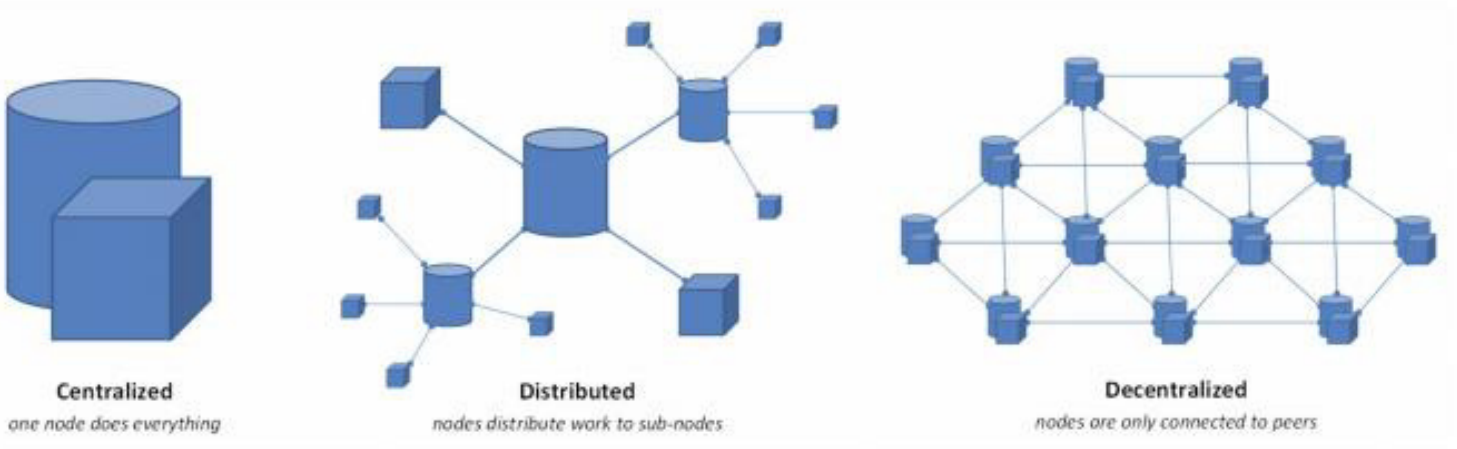
Per ottenere i benefici attesi dalla blockchain c'è quindi bisogno di un alto livello di **cooperazione** tra i partecipanti, che si può però tradurre in un sistema che porti a risparmio del lavoro e che sia meno soggetto ad errori

Architettura Centralizzata / Distribuita / Decentralizzata

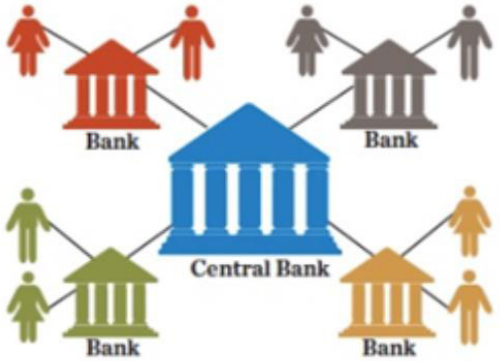
Centralizzata
Dati e Applicazioni in un unico nodo elaborativo

Distribuita
Dati e Applicazioni distribuiti su più nodi elaborativi cooperanti

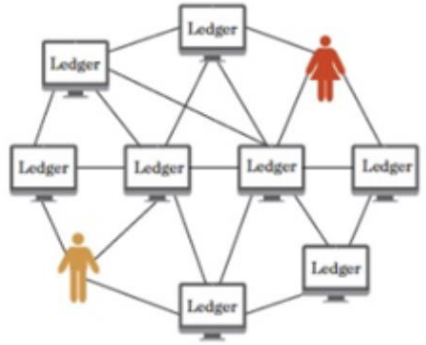
Decentralizzata
Tutte le operazioni possono essere svolte dai singoli nodi della rete (P2P)



ad esempio, nel caso dei sistemi di pagamento:



VS



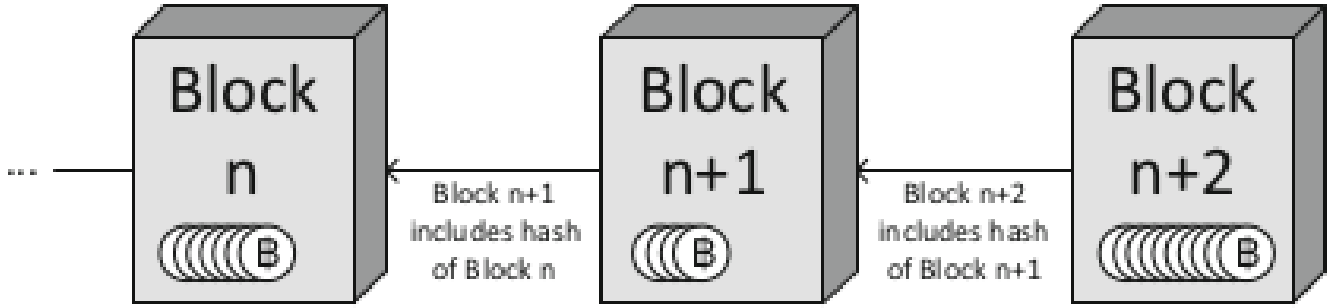
Distributed Ledger Technology (DLT)

Un **distributed ledger**, o registro distribuito, è un database distribuito su più macchine in cui possono essere registrate unicamente nuove transazioni ('**append-only**')

Blockchain (catena di blocchi)

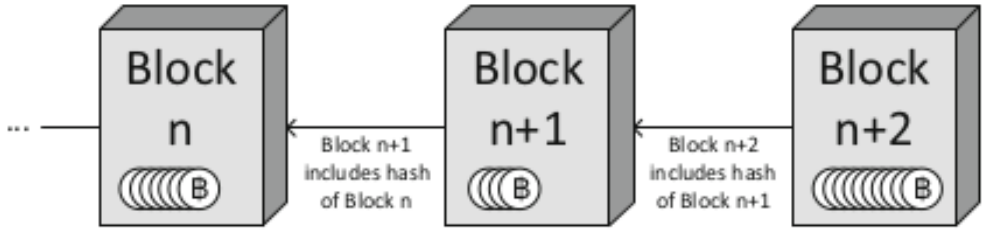
Una **blockchain** è un distributed ledger strutturato come una catena (*linked list*) di blocchi, ognuno contenente una serie di transazioni.

Nota: Ogni blockchain è un distributed ledger ma non il viceversa

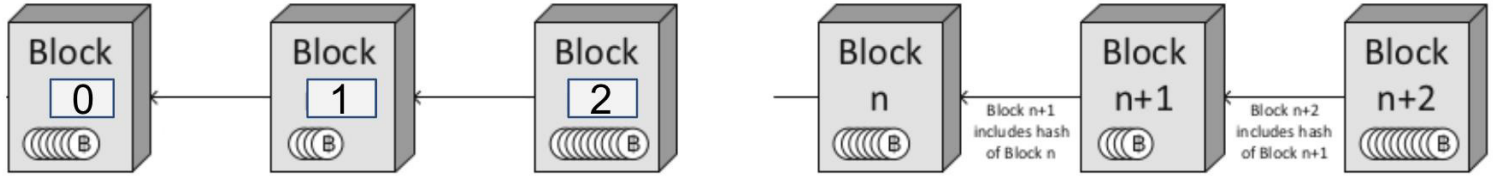


Come sono legati i blocchi

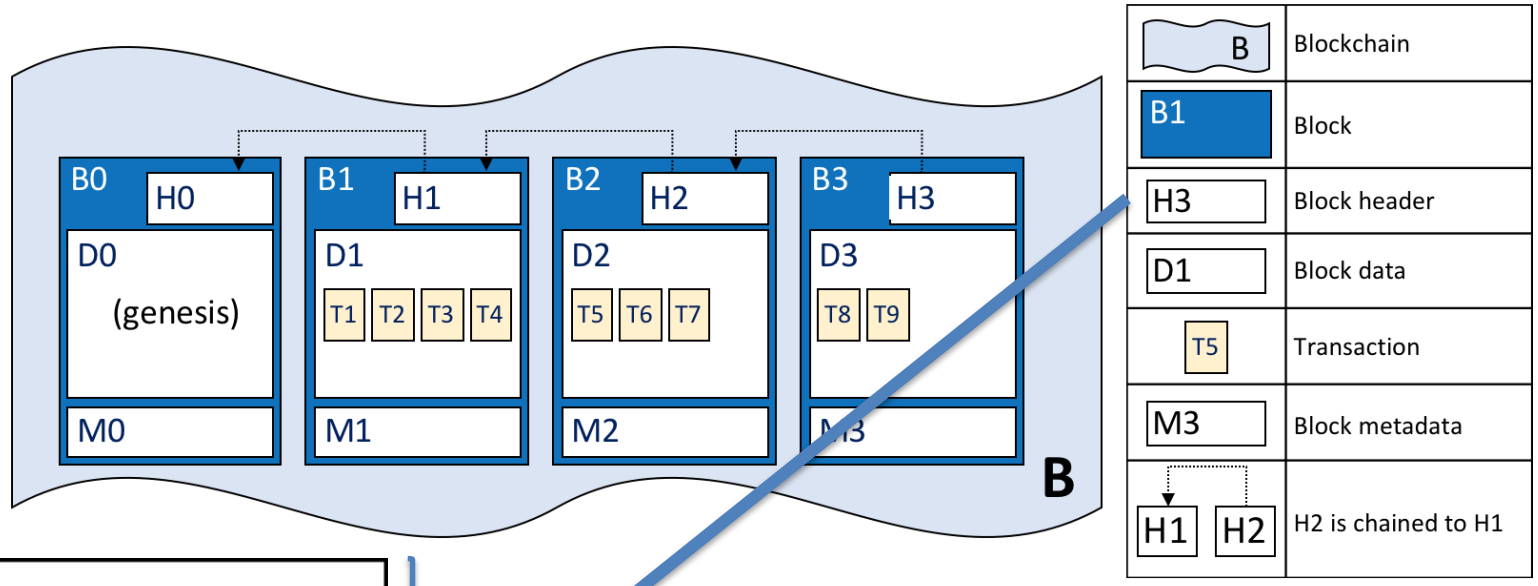
I blocchi sono connessi tramite meccanismi **crittografici** che creano un legame virtuale non modificabile



I blocchi sono **ordinati** secondo il *timestamp* di creazione



La struttura di un blocco



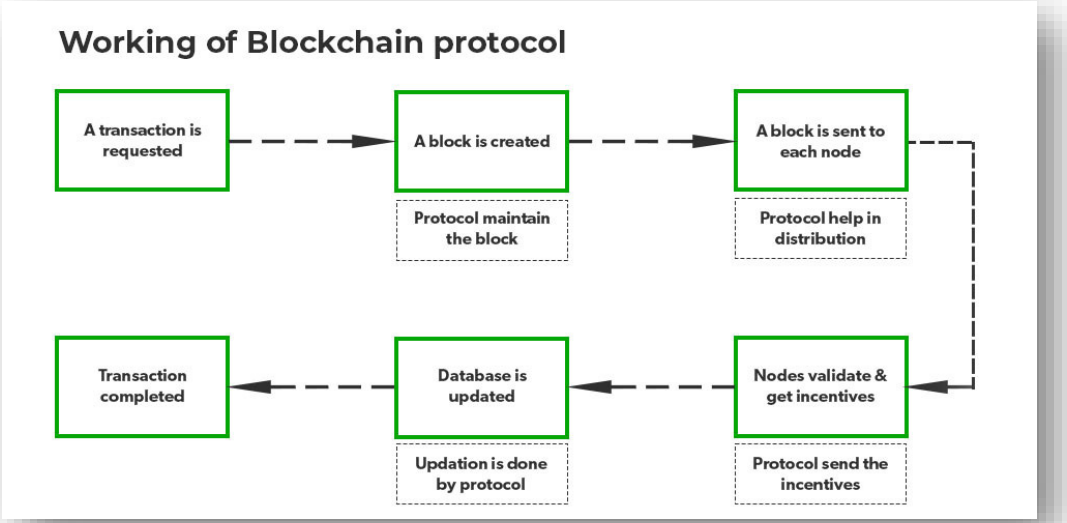
version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833

Esempio di Block Header in Bitcoin

Sistema Blockchain

Un sistema blockchain è composto da:

1. Una rete (**blockchain network**) composta da macchine, dette anche **nodi**;
2. Una struttura dati (**blockchain data structure**), ovvero la struttura di cosa contiene il registro replicato nella blockchain network.
3. Un **protocollo di rete** che definisce, tra l'altro:
   - Diritti
   - Responsabilità
   - Mezzi di comunicazione
   - Verifica
   - Validazione
   - Consenso

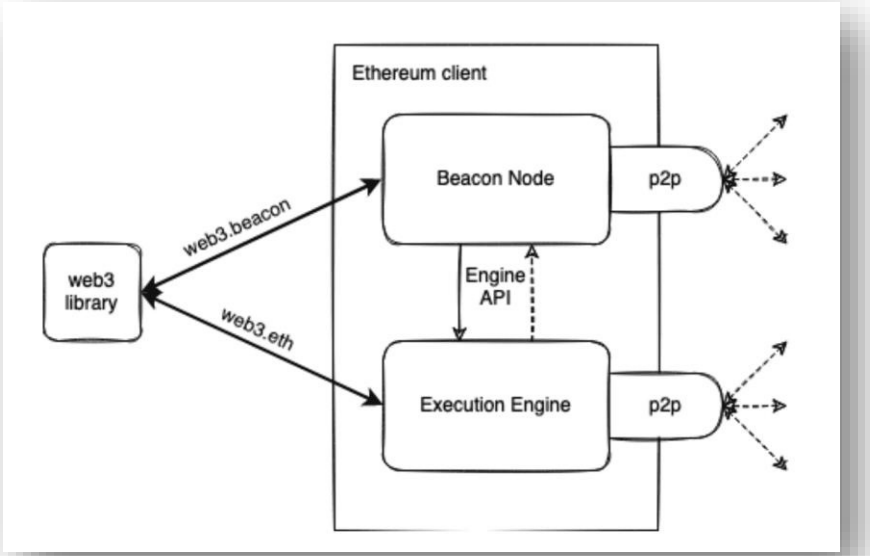


Fonte immagine: https://www.geeksforgeeks.org/blockchain-protocols-and-their-working/

Piattaforma blockchain

Una piattaforma blockchain è l'insieme delle tecnologie necessarie per operare su una blockchain:

- **Client software** per
  - operare sui nodi
  - accedere alla rete blockchain
  - memorizzare le chiavi private del proprio account
- **Data store** locale



Esempio di Ethereum client software con rappresentazione unificata del client di consenso (*beacon node*) e del client di esecuzione (*execution engine*) che ascolta e processa le transazioni nella rete

Caratteristiche della blockchain

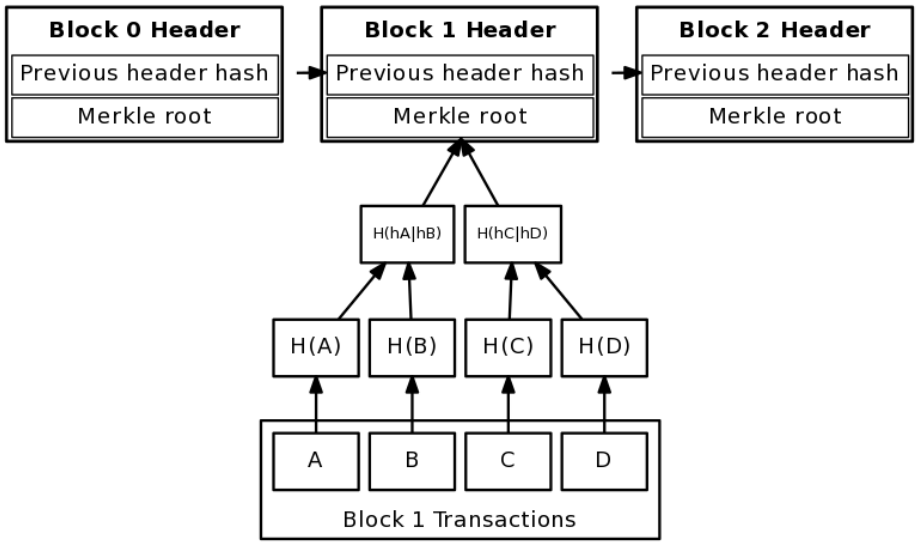
- Controlli appropriati di **integrità** per ogni transazione e blocco
- Meccanismi che usano strong encryption per **identificare** gli attori e controllare la loro **autorizzazione** ad aggiungere nuove transazioni
- **Validazione** delle transazioni effettuata da elementi *peer-to-peer* che richiede una serie di **incentivi** che promuovono la correttezza dei nodi partecipanti alla rete

- Correttezza e assenza di comportamenti anomali da parte del software di Sistema e dei protocolli tecnici

In realtà anche le blockchain possono essere soggette a vulnerabilità del software

Integrità: merkle tree

Il *merkle tree o hash tree* è una singola stringa che rappresenta la combinazione degli hash* delle transazioni che compongono un blocco



Merkle tree connecting block transactions to block header merkle root

Un client vuole verificare che una transazione faccia parte di un blocco:

*Ritrasmetto tutte le transazioni del blocco (**tanti dati**)*

oppure

*Ritrasmetto solo alcune combinazioni di hash per verificare la correttezza del merkle tree (richiede **meno operazioni e meno dati da trasmettere**)*

Merkle Proof

(*) il concetto di Hash function può essere approfondito qui: https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en

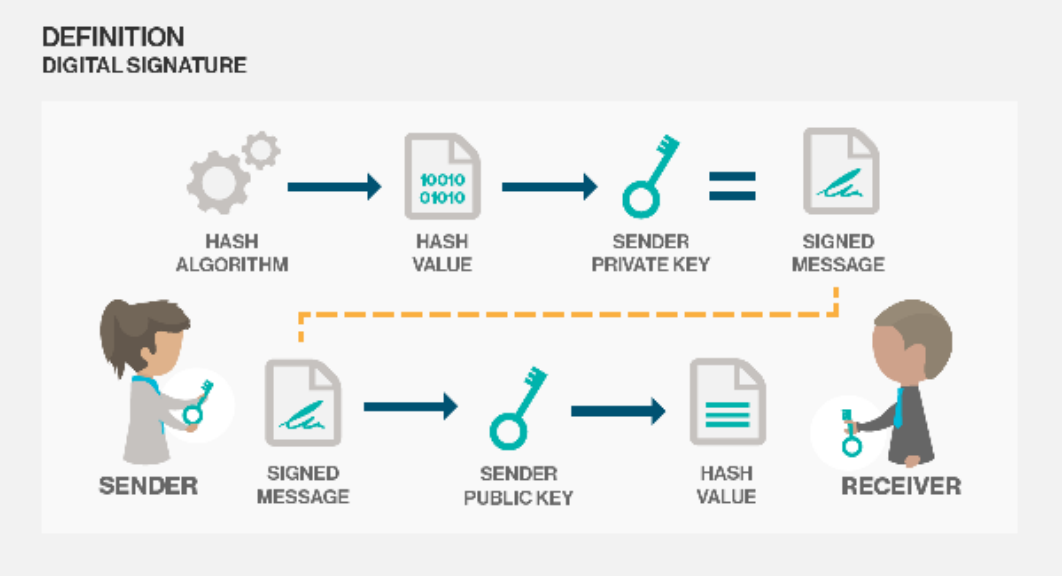
Identificazione e autorizzazione su blockchain

Ogni transazione viene firmata digitalmente dal mittente:

Due chiavi (chiave pubblica pk e chiave privata sk):

- se si usa una per cifrare, occorre l'altra per decifrare
- dall'una è praticamente impossibile dedurre l'altra

La chiave pubblica è resa di dominio pubblico, l'altra rimane privata (segreta) in possesso di chi l'ha generata



- Il mittente A cifra l'hash del messaggio con la sua chiave privata (ciò significa che il messaggio è in chiaro)
- Il destinatario B può "rivelare" l'hash solo usando la chiave pubblica del mittente A, e ciò gli dà la certezza che solo A abbia potuto calcolare e firmare l'hash perché solo A poteva conoscere la corrispondente chiave privata.
- Se l'hash del messaggio ricevuto è diverso dall'hash firmato, vuol dire che il documento è stato compromesso

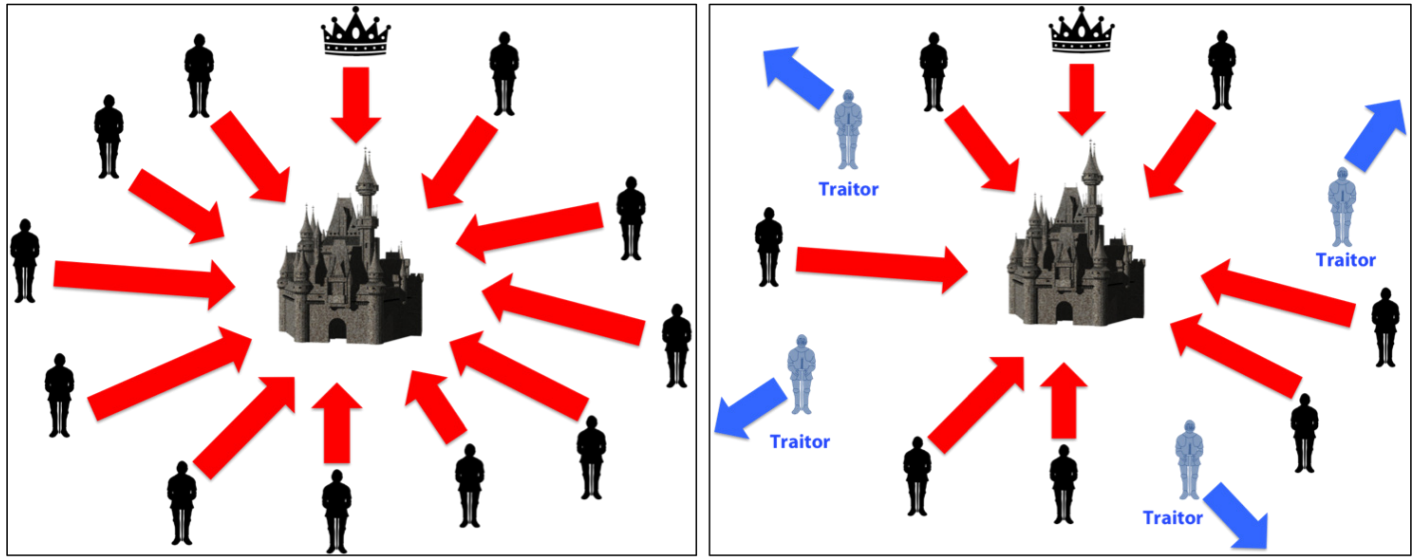
Chiave pubblica e privata identificano gli attori della blockchain

Correttezza dei nodi partecipanti: il problema del consenso

Poiché la blockchain è *distribuita*, è necessario stabilire un meccanismo di **consenso affidabile anche in caso di attori (nodi) inaffidabili**

Il problema è anche noto come **problema dei generali bizantini**

Approfondiremo successivamente le soluzioni proposte da blockchain differenti

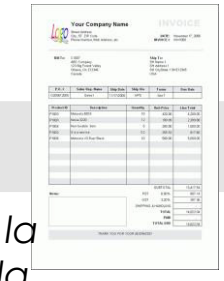


Coordinated Attack Leading to Victory **Uncoordinated Attack Leading to Defeat**

Leslie Lamport, Robert Shostak, and Marshall Pease. 2019. The Byzantine generals problem. Concurrency: the Works of Leslie Lamport. Association for Computing Machinery, New York, NY, USA, 203–226

Flusso di inserimento di una transazione nella blockchain

Alice vuole effettuare una transazione verso *Bob*



Alice compila la transazione e la firma digitalmente

La transazione viene validata e propagata ai nodi della rete

Ciascun nodo valida la transazione e la aggiunge ad una lista che porta alla formazione di un blocco

Una volta che viene 'completato' un blocco, i nodi procedono a dare il proprio consenso

Il blocco viene inserito nella blockchain e propagato tra i nodi

Bob riceve la transazione da Alice

Wallet

Se la blockchain conserva le transazioni, come faccio a sapere qual è il bilancio attuale di un soggetto?

- *ad es., Alice ha trasferito 50 BTC a Bob, il che significa che Alice aveva una disponibilità ≥ 50 BTC, ma dalla sola ultima transazione di Alice non è possibile capire a quanto ammonta il suo capitale attuale.*

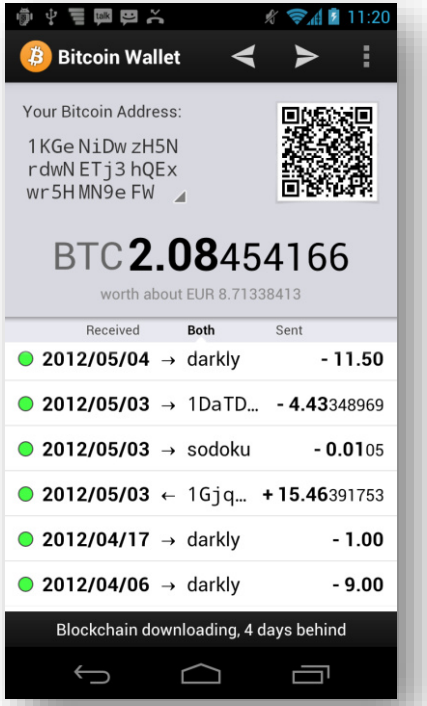
Possibili soluzioni:

1. Ricostruisco la catena delle transazioni e ricavo il valore attuale
   - quindi per ogni transazione utilizzo un
     - input – da quali transazioni deriva il patrimonio che sto per utilizzare;
     - e specifico un output - quanto sto trasferendo;

2. Utilizzo un registro degli stati ('stato patrimoniale')
   - **Wallet** è il registro dello stato di un singolo utente della blockchain.

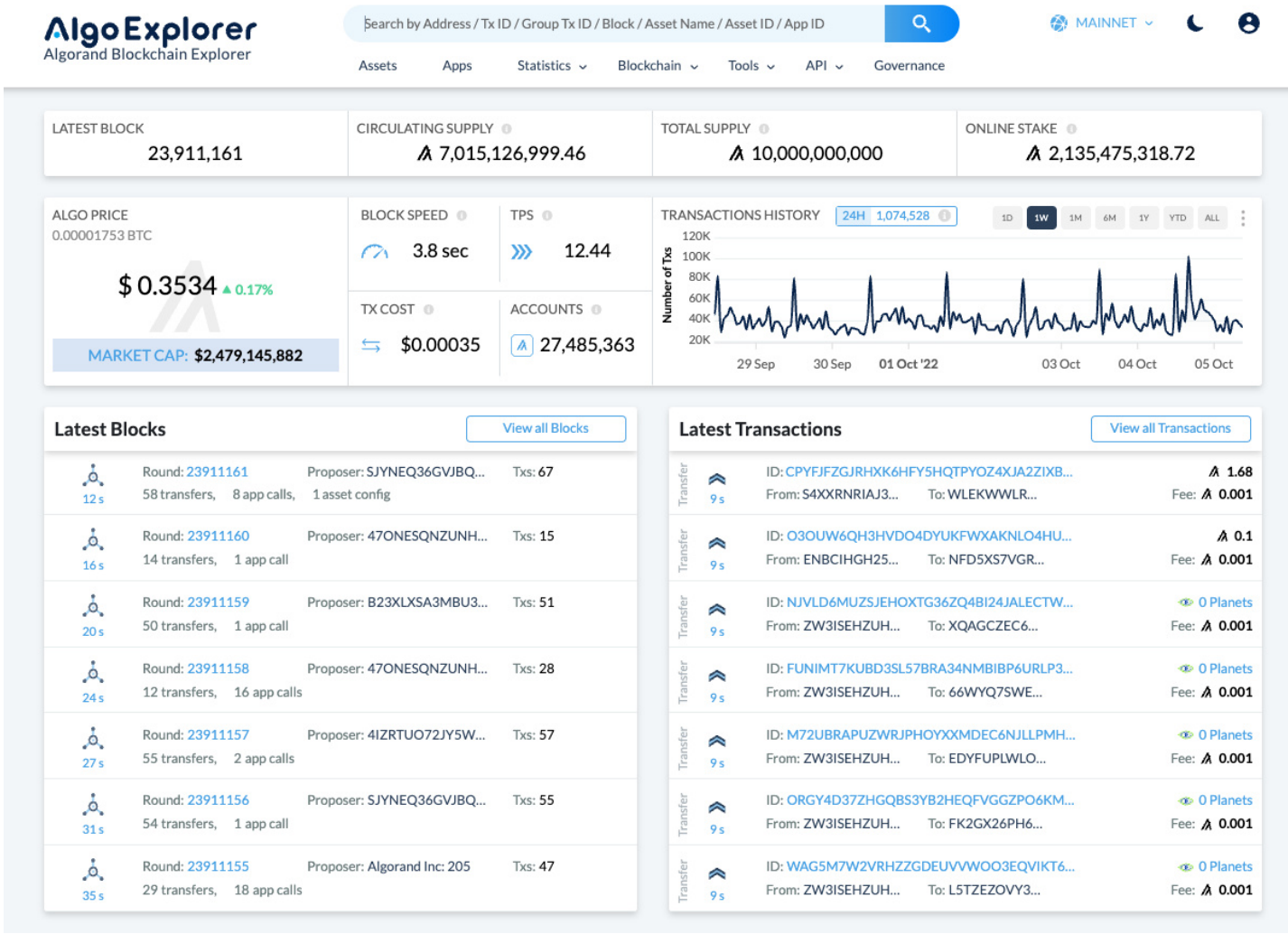
I wallet sono software che memorizzano le informazioni necessarie per la transazione.
Si basano sulla crittografia asimmetrica:

- **Chiave pubblica** : l'indirizzo pubblico del wallet
- **Chiave Privata** : usata per firmare digitalmente i contenuti del wallet

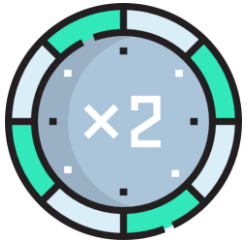


Blockchain explorer

La lista globale delle transazioni di una blockchain è solitamente pubblicata su un portale detto 'explorer', che permette la ricerca delle transazioni confermate nella chain



Criptovalute, fee & token



- Le **criptovalute** sono le valute alla base delle blockchain: Ether (ETH) è la valuta di Ethereum, Bitcoin (BTC) è la valuta di Bitcoin, Algo è la valuta di Algorand.
- Le **fee** (commissioni) sono correlate alle dimensioni di una transazione, non al suo valore: più dati (e con ciò vanno considerati anche gli smart contract che hanno più istruzioni) comportano commissioni più elevate. Allo stesso modo, calcoli più complessi, a seguito di invocazioni di smart contract, comportano commissioni più elevate.
- I **token** digitali possono essere creati e scambiati su blockchain. Generalmente i token vengono creati e gestiti utilizzando smart contract. Simile a una criptovaluta, ciascun token è controllato da un attore sulla blockchain. I token possono rappresentare azioni di una società, il diritto di beneficiare di guadagni futuri, o il diritto di utilizzare una risorsa.
- Gli **NFT** sono Token Non Fungibili, ossia Token che rappresentano asset digitali che hanno caratteristiche che non lo rendono sostituibile con nessun altro bene (e.g. un'opera d'arte, una casa, …)

Smart Contract

Gli smart contract sono dei programmi memorizzati nella blockchain, contengono delle funzioni che possono essere invocate tramite transazioni contenenti argomenti e parametri utili all'esecuzione di ciascuna di esse.

Gli smart contract possono essere utilizzati per gestire beni digitali o più in generale variabili di stato che vengono memorizzate sulla blockchain, permettendo di emulare operazioni simili ai contratti legali

Il codice di uno smart contract è deterministico e immutabile una volta pubblicato sulla blockchain

Quando uno smart contract viene invocato, ogni nodo effettua l'esecuzione del codice contenuto in esso.

L'esecuzione è costosa e aumenta con la complessità del software

L'evoluzione della blockchain

- Lo sviluppo della blockchain è avvenuto in 3 fasi principali:
- **Blockchain 1.0**: La blockchain si applica principalmente alla **valuta digitale**.
  - Bitcoin è stato proposto nel 2008 da S. Nakamoto realizzando una transazione di pagamento decentralizzata per le valute digitali.
  - Bitcoin utilizza l'algoritmo di consenso proof-of-work. Sulla sua base sono nate altre valute digitali come Dogecoin e Litecoin.
- **Blockchain 2.0**: Viene introdotto il concetto di **smart contract**, ampliando notevolmente il campo di applicazione della blockchain.
  - Ethereum fornisce una piattaforma affidabile ambiente di programmazione smart contract, che consente agli utenti di scrivere contratti adatti e intelligenti in base alle proprie esigenze e alla propria applicazione scenari, come il voto di crowdfunding azionario e il trading di titoli e emissione.
- **Blockchain 3.0**: Con il rapido sviluppo della blockchain, la blockchain conferma il **diritto di proprietà delle informazioni** che rappresentano il valore su Internet.
  - La blockchain può tracciare e controllare le risorse mentre le negozia. In genere, il settore della blockchain non si limita a denaro, economia e mercati
  - Si è esteso ad altre aree richieste, come la salute, la certificazione di identità, la logistica e votazione.
  - Attualmente, l'ambito dell'applicazione blockchain è su tutto il livello sociale

Il problema del consenso e il trilemma della blockchain

- Vitalik Butherin (fondatore di Ethereum) formulò la definizione di TRILEMMA blockchain:

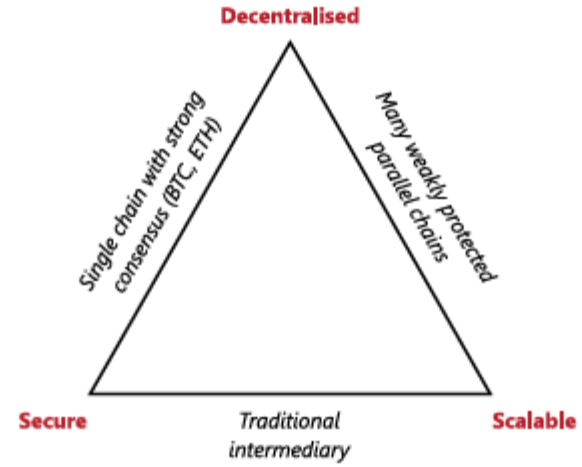
è difficile costruire una blockchain che garantisca le seguenti 3 proprietà:

Decentralizzazione *- capacità del sistema di facilitare la partecipazione alla rete avendo accesso a risorse limitate (laptop, virtual private server,...);*

Scalabilità *- capacità del sistema di adeguarsi (in termini computazionali) al fine di mantenere un limite massimo del numero di transazioni processate (max throughput) maggiore rispetto ai requisiti dell'ecosistema;*

Sicurezza *- non vulnerabilità ad attacchi da sorgenti esterne*

Buterin's "scalability trilemma" Graph 3



Sources: Auer et al (2021); Buterin (2021).

Il Trilemma è strettamente legato alla modalità con cui viene risolto il problema del consenso in una blockchain

Proof of Work

Proof-of-work (**PoW**): i nodi della rete che partecipano al consenso devono risolvere un puzzle crittografico basato sulla risoluzione di *One Way Function,* ossia funzioni che sono difficilmente reversibili. Il puzzle, seppure facile da verificare, richiede un grande sforzo computazionale (ecco perchè si chiamano **MINERS**) e tempo variabile.

- Ogni transazione è propagata a tutti i nodi
- Ogni nodo raggruppa le transazioni in un blocco e prova a risolvere la PoW
- Chi risolve il problema inserisce il blocco nel distributed ledger e lo comunica agli altri nodi
- Gli altri nodi riconoscono il blocco dopo aver verificato la soluzione e la validità delle transazioni.
- Il nodo che ha risolto la PoW ottiene una ricompensa (che può essere sia un incentivo della rete che una tassa sulla transazione).

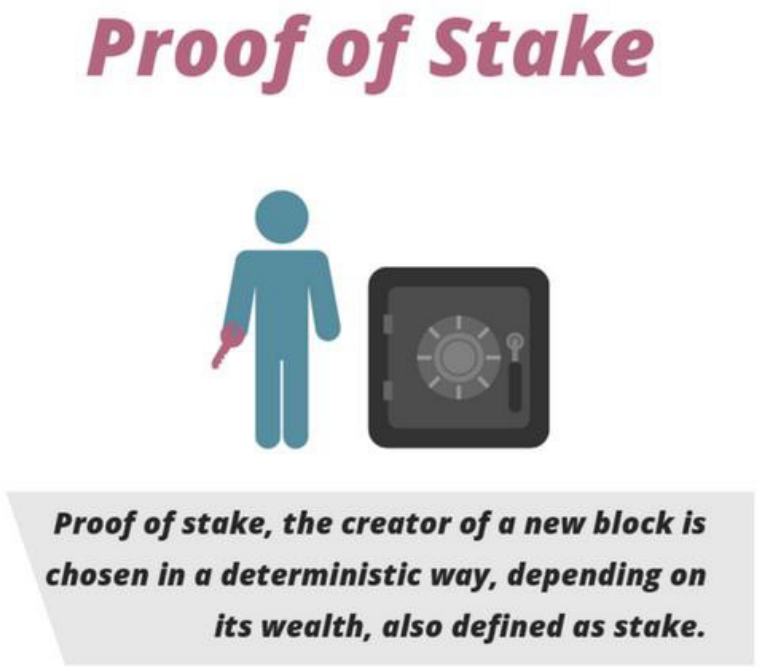
Proof of Stake

Proof of Stake (**PoS**) è una formula di consenso partecipata solo da alcuni nodi della rete blockchain, che non necessariamente svolgono un lavoro di calcolo oneroso ma che godono di particolare facoltà nella rete grazie alla loro situazione di benessere patrimoniale

Il concetto di base è che chi detiene una maggior quantità di criptovaluta non ha interesse a compromettere la rete, pertanto è ragionevolmente deputato a comportarsi onestamente nel processo di validazione.

La PoS assume varie declinazioni che possono essere basate su:

- Selezione randomica dei possessori di criptovaluta
- Anzianità nel possesso di una certà quantità di criptovaluta
- …
- Nei casi di blockchain private si può avere **Proof of Authority** (in cui nodi deputati stabiliscono il consenso)

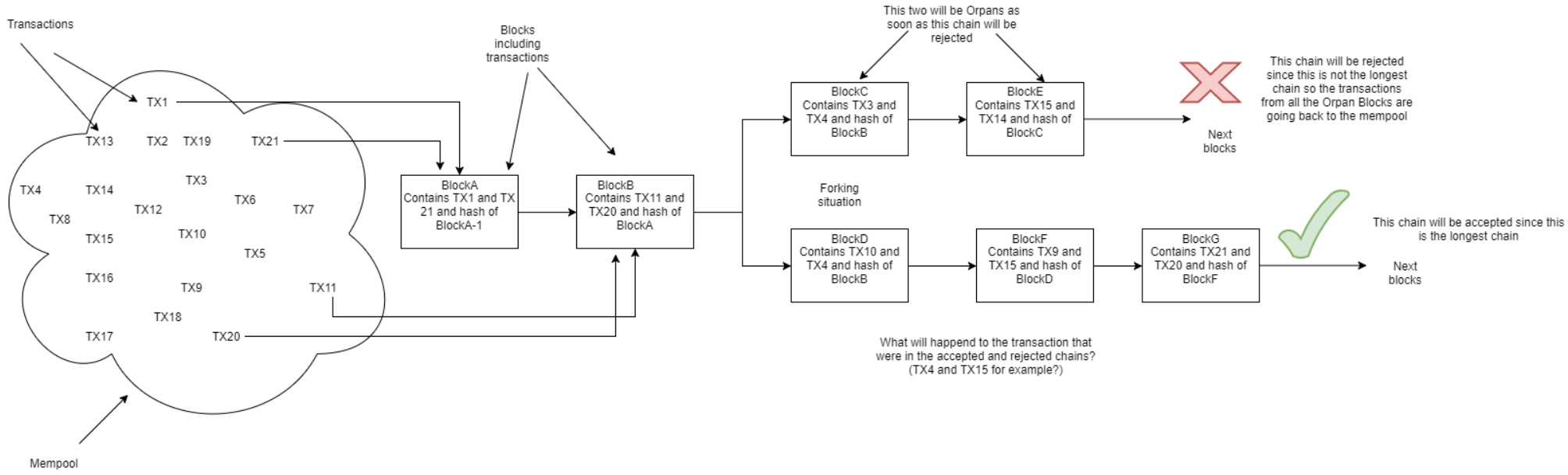


Blockchain e scalabilità

- Limiti di scalabilità dovuti a
  - La dimensione dei dati sulla blockchain
    - a causa della replicazione globale sui registri dei nodi
  - La velocità con cui vengono eseguite le transazioni.
    - *Mainstream public blockchains* gestiscono in media tra le 3 e le 20 transazioni al secondo. Circuiti come VISA, ne gestiscono 1700 al secondo.
  - La latenza nella trasmissione dei dati.
    - La larghezza di banda a disposizione dei nodi che partecipano al consenso impatta sia sulla propagazione dei blocchi che devono essere aggiunti sui registri locali (maggiore è la latenza e maggiore è la probabilità di fork) sia sul numero di transazioni che compongono un blocco (ad es. in Bitcoin la dimensione di un blocco è di 1 MB). Va inoltre tenuto da conto la latenza dovuta alla tipologia di consenso (*1h Bitcoin [con almeno 6 blocchi confermati]– 3 min Ethereum [con almeno 12 blocchi confermat*i])

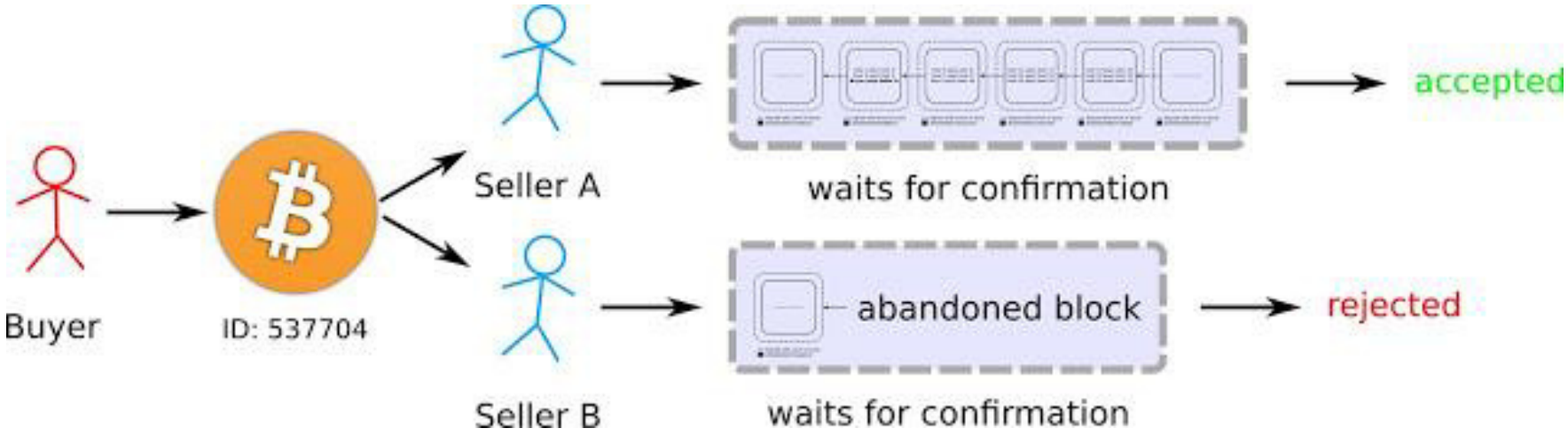
Sicurezza della blockchain: i fork

- I **fork Blockchain** si verificano quando due miners/validators trovano e pubblicano indipendentemente un nuovo blocco che fa riferimento allo stesso blocco precedente
- Dipendentemente dal tipo di blockchain, effettuare il *commit* di una transazione non significa averne la *confirmation*
- I nuovi blocchi verranno aggiunti sempre alla catena più lunga

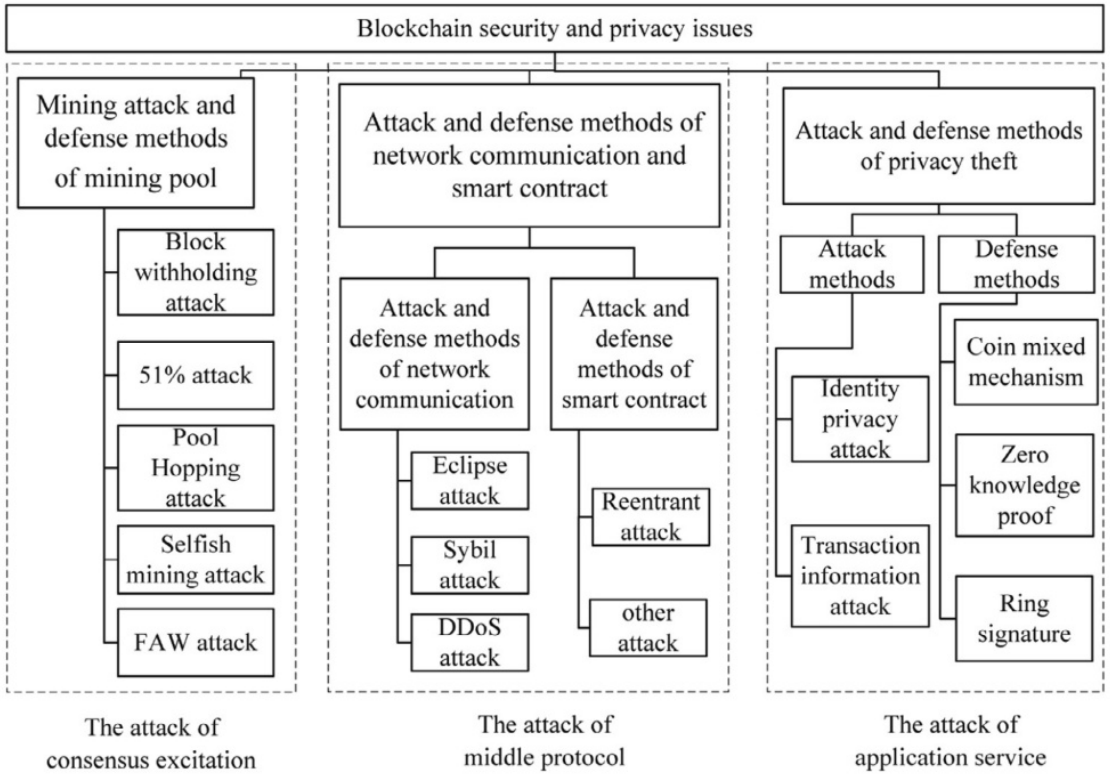


Effetto dei fork: double spending

- Nelle blockchain, un compratore può spendere la stessa quantità di criptovaluta in due transazioni diverse
- E' consentito, in quanto un fork dopo un po' cessa di esistere
- Un attore malevolo può usare il double spending a suo vantaggio



Sicurezza nella blockchain



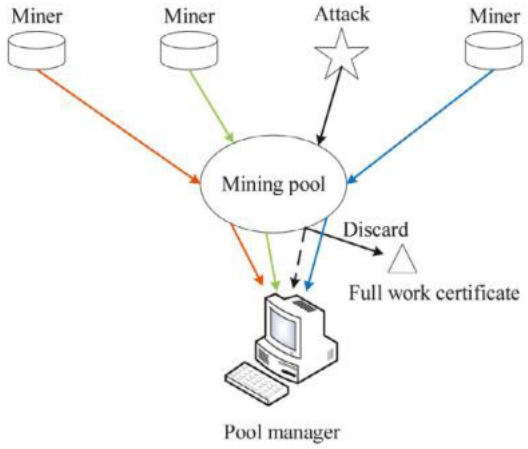
Gli attacchi alla blockchain possono essere classificati come

- **Attacchi con eccitazione del consenso**
  - Quando l'attaccante in qualche modo riesce ad ottenere un compenso aggiuntivo intereferendo con il consenso
- **Attacchi ai protocolli nel mezzo**
  - Quando l'attaccante agisce sui nodi di comunicazione o sugli smart contract
- **Attacchi al servizio applicativo**
  - Quando l'attaccante sfrutta vulnerabilità del servizio applicativo per recuperare informazioni private degli utenti

Chen et al., «A survey on blockchain systems: Attacks, defenses, and privacy preservation», High-Confidence Computing 2 (2022), Elsevier

Esempio di attacco con *block witholding*

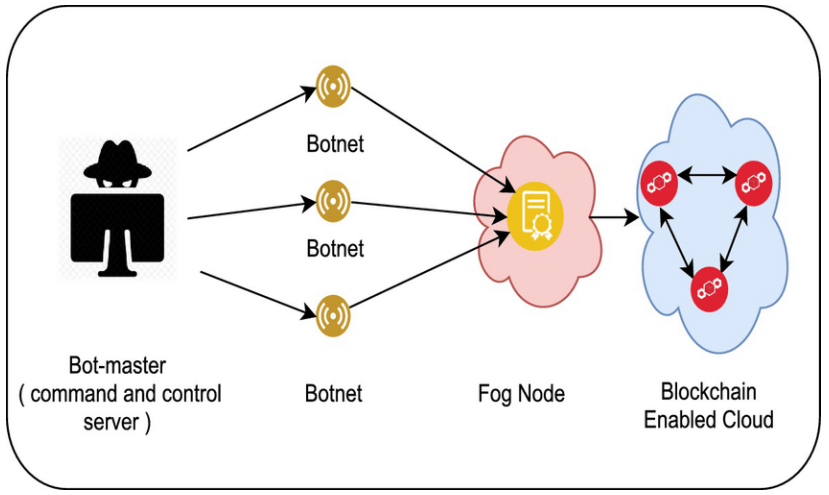
- **Precondizioni**: più attori concorrono in un pool a calcolare la PoW mettendo a disposizione le proprie risorse di calcolo
- **Attacco**: uno o più miner disonesti in un pool calcolano la *complete proof of work* ma non la comunicano al pool
- **Obiettivo**: impedire ad un pool di ottenere la ricompensa
- **Difese**: rendere partial proof of work e complete proof of work indistinguibili ai miner, minimizzare il profitto di attori malevoli



Altri esempi di attacchi con eccitazione del consenso possono essere: attacco con 51% della capacità computazionale della rete; attacco con partecipazione a più pool;…

Esempio di attacco con dDOS

- **Precondizioni**: l'attaccante controlla più nodi della rete
- **Attacco**: l'attaccante sovraccarica il target (un miner o un validator) di informazioni false
- **Obiettivo**: impedire a uno o più miner di portare a termine validazioni e transazioni
- **Difese**: classificatori di comportamento (intrusion detection systems)



Altri esempi di attacchi che sfruttano la rete possono essere il sybil attack (l'attaccante impersonifica attori diversi) o l'eclipse attack (parte della rete viene «eclissata» nelle comunicazioni)

Esempio di attacco alla privacy

- **Attacco**: l'attaccante ottiene la chiave privata di un wallet, o ne intercetta gli scambi, sostituendosi al mittente (replay) o fingendosi un altro utente (impersonation).
- **Obiettivo**: ottenere il controllo di un wallet
- **Difese**: educare gli utenti, utilizzare sistemi di *intrusion detection*

Smart Contract vulnerabilities

- Gli smart contract sono programmi informatici e come tali possono essere soggetti ad errori di progettazione del codice
  - e.g.: in solidity (Ethereum smart contract) è prevista la possibilità di utilizzare dei cicli (*loop*) di calcolo, tuttavia, in caso di una mancata analisi del codice, potrebbero verificarsi dei casi in cui le condizioni di uscita dal *loop* non si verifichino e quindi l'esecuzione dello smart contract (su tutte le EVM) verrebbe iterata ripetutamente… per tale motivo Etherum prevede un **limite di consumo di gas**, così da interrompere le esecuzioni di codice che eccedono un numero di operazioni prefissato.
- Un attacco tipico agli smart contract mal progettati è la **re-entrancy** causata dalla concessione a smart contract esterni di fare invocazioni ricorsive a funzioni di trasferimento dei fondi:
  - e.g.:
    1. Un primo smart contract assolve alla funzione di custode della criptovaluta
    2. Un attaccante deposita una quantità di criptovaluta sul primo smart contract
    3. Lo stesso attaccante chiede al primo smart contract di trasferire i fondi verso uno smart contract 'malizioso', il quale riceverà i fondi e invocherà ricorsivamente sul primo smart contract la stessa funzione di trasferimento dei fondi, operazione che avrà successo fintanto che non verrà aggiornato il *balance* dell'attaccante -> lo smart contract 'malizioso' prosciugherà il deposito del primo smart contract
- **RIMEDI:** usare strumenti di Vulnerability Assessment oppure evitare linguaggi di programmazione che evitino a priori le precondizioni di vulnerabilità (e.g. la chiamata verso smart contract esterni).

Governance delle blockchain

Chi effettua le scelte tecniche della blockchain? Chi aggiorna e corregge il protocollo?

Partiamo dal fatto che esiste una *Blockchain community*

Users	sono coloro che effettuano le transazioni sulla blockchain. Il loro interesse è il mantenimento del registro distribuito e, nel caso di asset digitale, preservare o aumentare il valore del loro patrimonio. Il costo delle transazioni deve essere inferiore al valore della transazione (sia essa di un asset digitale o meno)
Miners / Validators	In cambio del loro sostegno alla rete P2P, i nodi che ricoprono questo ruolo ricevono «*transaction fees*» oppure «*block rewards*». Tenderanno quindi a favorire i cambiamenti che possono aumentare o stabilizzare il valore del loro patrimonio.
Developers	Sono coloro che sviluppano il protocollo della blockchain e ne assicurano la manutenzione, correttiva, adeguativa o evolutiva, impattando su tutta la comunità. La loro attività è ripagata dal successo della rete blockchain di cui sono artefici. Qualora la rete blockchain sia legata a transazioni di un digital asset, i developers sono artefici dell'aumento del proprio patrimonio; in altri casi sarebbe opportuno definire strategie per il mantenimento a lungo termine della parte di sviluppo software.

"Miners want fees, devs want controlled implementation of change as well as increasing network success, and businesses want whatever is best for their bottom line"

Blockchain pubblica & permissionless

Una blockchain **pubblica** e **permissionless** ha le seguenti caratteristiche:

È costituita da una *open network* dove i nodi possono unirsi o sganciarsi quando vogliono, senza dover chiedere il permesso a nessuno;

Tutti i *nodi full* della rete possono verificare ogni nuovo dato aggiunto alla struttura dati, pertanto possono verificare blocchi, transazioni e gli effetti delle transazioni;

È caratterizzata da un protocollo che include **meccanismi di incentivazione** utilizzati per assicurare il corretto funzionamento della blockchain, ossia che le transazioni vengano validate e aggiunte al registro distribuito o vengano scartate se ritenute invalide.

Blockchain pubblica & permissioned

Una blockchain **pubblica** e **permissioned** si differenzia da una blockchain pubblica e permissionless poichè:

una o più **autorità** stabiliscono chi può partecipare al Sistema blockchain, definendo quali sono i nodi che:

- hanno il *permesso di proporre una transazione*
- hanno il *permesso di partecipare al consenso* e quindi di scrivere sul registro distribuito
- hanno il *permesso di sola lettura* del registro distribuito

Blockchain privata

Una blockchain privata è gestita da una singola autorità o da un consorzio

I gestori hanno totale controllo sui nodi che hanno accesso alla blockchain

La blockchain privata può essere permissionless o permissioned, ma in ogni caso esiste una forma di controllo di accesso a priori (ad esempio tramite l'utilizzo di una virtual private network o all'interno di una LAN)

La blockchain privata viene generalmente utilizzata in caso sia necessario garantire specifiche performance in un ambiente chiuso

Confronto tra le scelte di controllo della blockchain

		Permission-less		Permissioned	
Public	Immutability	+++	(#Nodes, Consensus, Topology)	Immutability	++
	Integrity	+++	(#Nodes, Consensus, Topology)	Integrity	++
	Transparency	++	(Access control)	Transparency	++
	Availability	+++	(#Nodes, Topology)	Availability	++
	Performance	+	(Consensus, latency)	Performance	++
	Cost Efficiency	+		Cost Efficiency	++
Private	Immutability	+		Immutability	+
	Integrity	+		Integrity	+
	Transparency	+		Transparency	+
	Availability	+		Availability	+
	Performance	+++		Performance	+++
	Cost Efficiency	+++		Cost Efficiency	+++

Xu, Xiwei & Weber, Ingo & Staples, Mark. (2019). Architecture for Blockchain Applications

Bitcoin

Consenso	Categoria	Reward
Proof of Work	Public & Permissionless	Block creation + fees

Funzionamento:

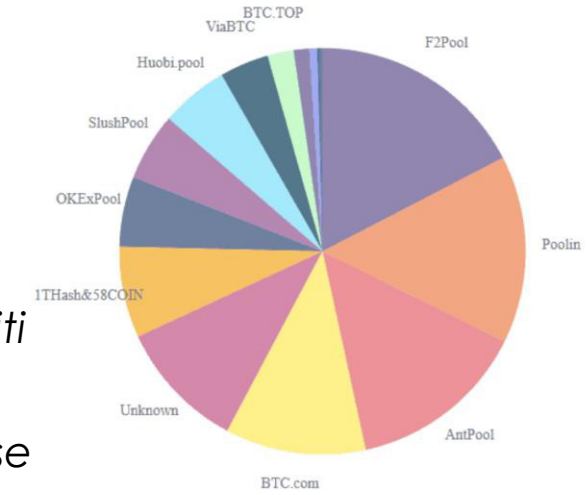
1. *Tutti i nodi vengono a conoscenza delle nuove transazioni*
2. *Le transazioni sono raggruppate in un blocco (se valide)*
3. *Ogni nodo risolve un problema crittografico, comunicando a tutti gli altri nodi la propria prova di risoluzione*
4. *Tutti i nodi verificano la prova della soluzione del problema crittografico comunicata in precedenza*
5. *Il nuovo blocco viene aggiunto alla catena*

Effetti:

crescita lineare dello sforzo computazionale:

Il mining richiede costi crescenti a causa dei requisiti hardware per l'elaborazione

I miners si uniscono ai pool (per condividere le risorse computazionali)



May 2020: Hashrate distribution by mining pool.
Image credit: blockchain.com

Forza di calcolo concentrata in pochi mining pool: la blockchain perde *decentralizzazione*

S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2009

Ethereum

Consenso	Categoria	Reward
Proof of Work	Public & Permissionless	Block creation + fees

- **PoW** richiede un elevato costo computazionale (quindi la partecipazione come **miner** richiede un ingente investimento economico)
- Ciò comporta una elevata latenza per la creazione di un blocco, per questo tale protocollo originale è stato modificato fondando Ethereum Casper
- Tra le principali caratteristiche abbiamo:
- Introduzione del concetto di **smart contract**
  - GAS Price: Il prezzo del GAS è l'unità fondamentale di calcolo, in genere **una fase computazionale costa 1 gas**, ma alcune operazioni costano quantità di gas più elevate perché sono computazionalmente più onerose
- Documentazione abbondante per lo sviluppo con **Solidity**
- Definizione di **wallet interni**. Ciò permette di definire nuovi token, trasferibili e consultabili unicamente con chiamate a smart contract.

Ethereum: Internal transactions

To:	Contract 0xd0a6e6c54dbc68db5db3a091b171a77407ff7ccf (EOSCrowdsale)
Token Transfer:	312.603736665917934133 ($4,557.01) EOS Token from 0xd0a6e6c54dbc68... to 0x14138ccf3a82375...
Value:	0 Ether ($0.00)
Gas Limit:	90000
Gas Used By Txn:	81253
Gas Price:	0.00000005 Ether (50 Gwei)
Actual Tx Cost/Fee:	0.00406265 Ether ($2.84)
Nonce & {Position}:	53 | {166}
Input Data:	Function: claim(uint256 day)

Indirizzo dello smart contract
Quantità di token trasferiti
Quantità di ETH trasferiti
Dati legati al consumo di GAS per questa transazione
Fee
Nonce
Payload (invocazione)

Transactions | Internal Transactions | Token Transfers | Comments

Internal Transactions as a result of Contract Execution

Latest 3 Internal Transactions

ParentTxHash	Block	Age	From		To	Value
0xdde53038c4f1f8f...	4680419	158 days 6 hrs ago	0xf3ba2ed79a87b7f...	→	0xbe2b28f87033...	0.49 Ether
0xb844409a3e938fe...	4680417	158 days 6 hrs ago	0xe213bdf9dfc0bf4...	→	0xbe2b28f87033...	0.49 Ether
0x4870ac83c8ae6c...	4591019	172 days 23 hrs ago	0xacdaf869fe5c09a...	→	0xbe2b28f87033...	0.94 Ether

Le **invocazioni agli smart contract** sono etichettate come transazioni interne

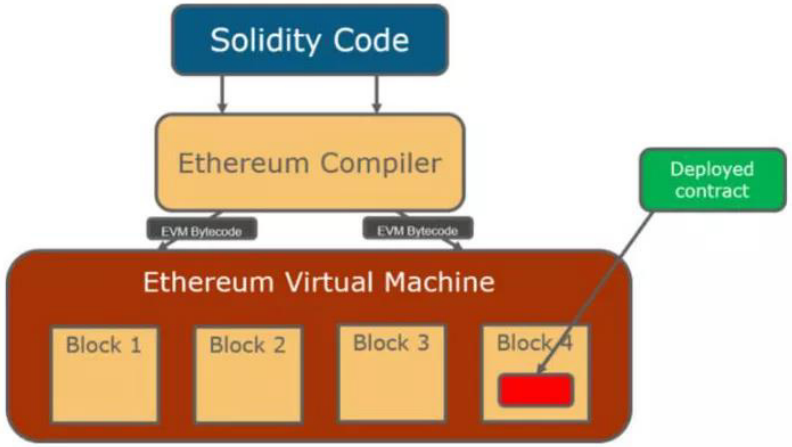
https://etherscan.io/

Ethereum: EVM

- La **Ethereum Virtual Machine**, spesso abbreviata attraverso l'acronimo EVM, è il **centro di calcolo che permette l'esecuzione di smart contract** al di sopra della piattaforma Ethereum.
- Lo **stato di Ethereum Virtual Machine (EVM) è memorizzato nella blockchain** di Ethereum.
- **Ogni nodo esegue un EVM locale**. Quando un account desidera eseguire una funzione di uno smart contract, emette una transazione che viene trasmessa alla rete.
- Ogni nodo esegue la transazione sul suo EVM locale e lo memorizza, insieme al nuovo stato calcolato, nella blockchain.

Solidity

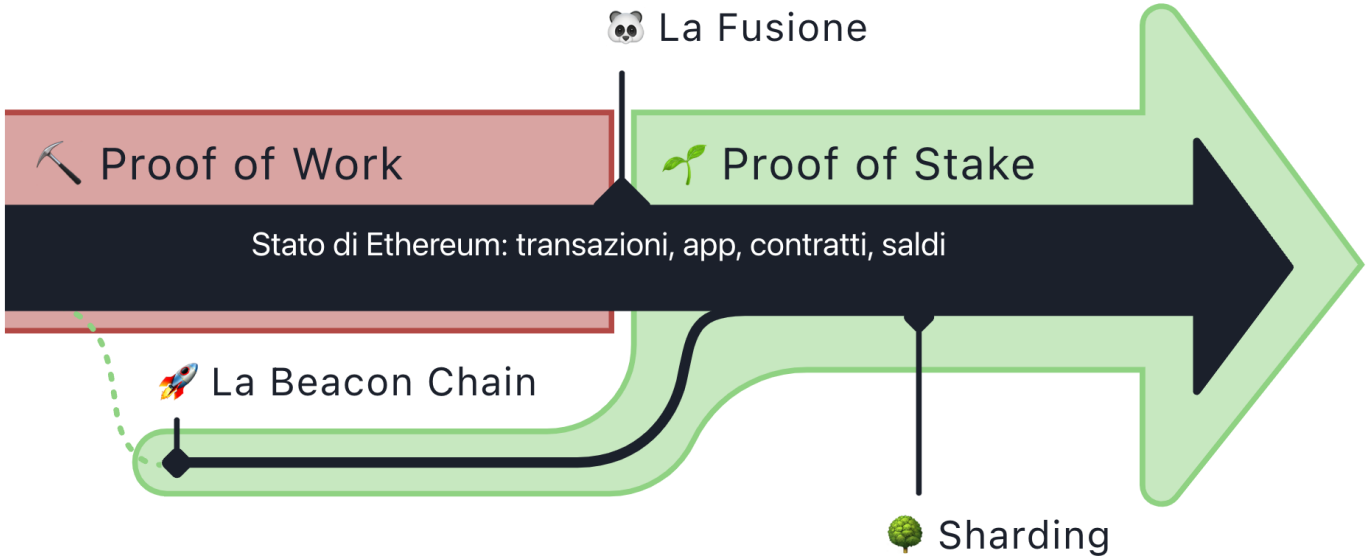
- Linguaggio per lo sviluppo di smart contract su Ethereum
- Turing complete
- Object-oriented
- Tipizzato
- Concetto di ereditarietà
- Diverse librerie di ausilio



https://ethereum.org/it/developers/

Merge di Ethereum

- La Rete principale di Ethereum usa il *Poof of stake*, ma non è sempre stato così.
- La transizione dal meccanismo originale di Proof of Work al Proof of stake è stata chiamata **La Fusione (The merge)**.
- La Fusione si riferisce al momento in cui la Rete principale originale di Ethereum è divenuta parte di una blockchain di Proof of stake separata, detta *Beacon Chain*, ora esistente come un'unica catena.
- La Fusione ha ***ridotto il consumo energetico*** di Ethereum di circa il 99,95%.



15 settembre 2022

Algorand

Consenso	Categoria	Reward
Pure Proof of Stake	Public & Permissionless (anche se il set validatori è ristretto)	Governance participation

Caratteristiche fondamentali:

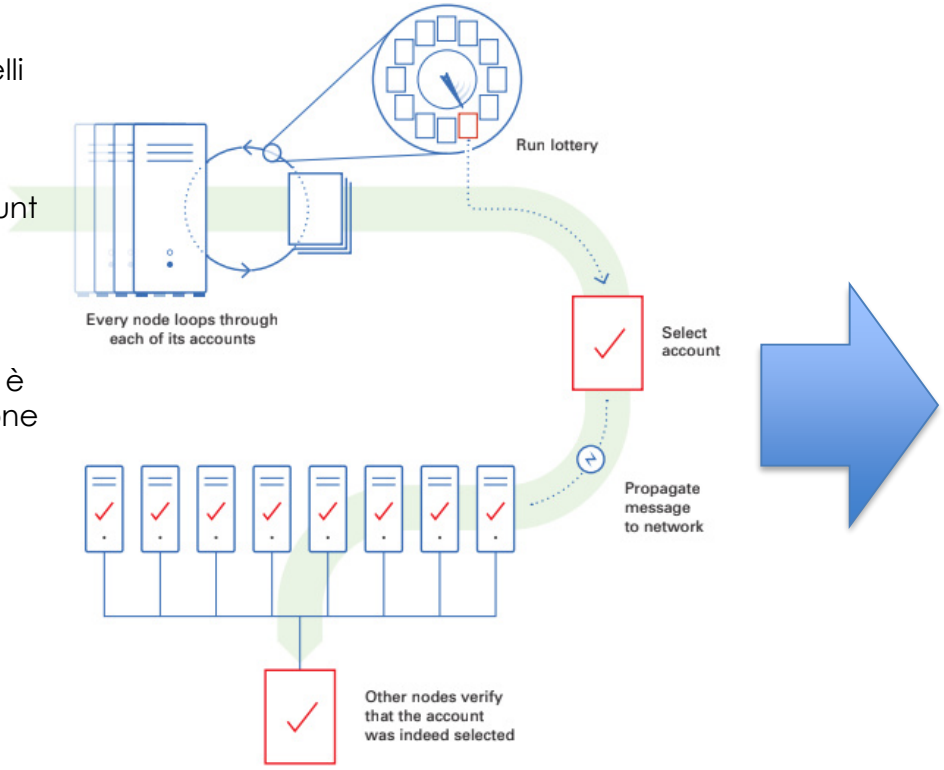
- **Pure Proof of Stake** (nuova modalità di risoluzione del problema bizantino)
- Immediate Transaction Finality
  - La probabilità di fork su algorand è pari a 10^(-18) , evitando il double spending
- Self-Selection
  - I validatori di un blocco non sono mai gli stessi, vengono scelti in maniera randomica attraverso opportune VRF (Verifiable Random Function)
- User replaceability
  - Siccome gli utenti sono scelti in maniera randomica ed indipendente ogni round di consenso e, il messaggio viene inoltrato prima che l'utente sappia di partecipare, un exploit di questo protocollo risulta probabilisticamente molto basso
- Scalability
  - Dal punto di vista computazionale il protocollo risulta molto efficiente
- Soluzione al trilemma della blockchain
  - favorisce la decentralizzazione, è scalabile ed è difficile da pilotare nei processi di validazione

Come funziona il PPoS

Block proposal

- Ogni nodo *itera i suoi account*, per trovare quelli online e con una valida partecipation key
- Individuato il set di account viene scelto randomicamente un account

  La scelta randomica è analoga all'esecuzione di una **lotteria**, realizzata attraverso l'uso delle VRF (Verifiable Random Function)
- Una volta selezionato, l'account trasmette la prova che è stato selezionato ed il blocco proposto

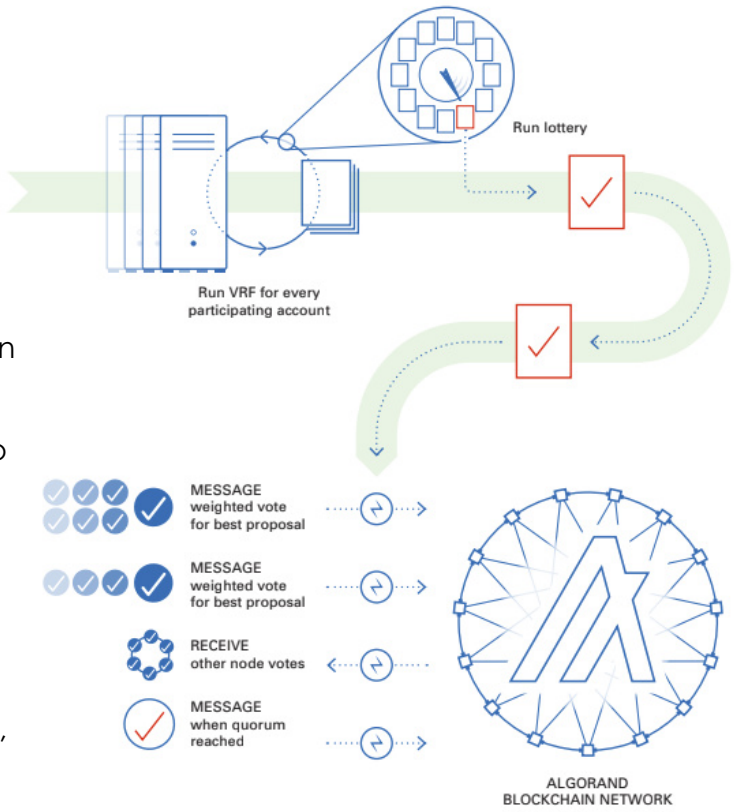


Jing Chen, Silvio Micali, «Algorand: A secure and efficient distributed ledger», Theoretical Computer Science, Volume 777, 2019

Soft Vote & Certify Vote

Bisogna scegliere un solo blocco tra quelli proposti:

- Ogni nodo eseguirà la VRF per sapere se fa parte del comitato di '**soft vote**'
- Ogni account scelto avrà un **voto ponderato** proporzionale al suo stake in Algo
- Si vota su un singolo blocco tra quelli proposti, scelto deterministicamente
- Al raggiungimento del quorum dei voti su un blocco si chiede ad un **comitato di certificazione,** selezionato analogamente, di votare la conferma del blocco, che viene quindi inserito nella chain



Algorand: strumenti per lo sviluppo di soluzioni

https://developer.algorand.org/

- **Algorand Standard Asset**: creazione di risorse on-chain (NFT) che beneficiano della stessa sicurezza, compatibilità, velocità e facilità d'uso degli Algo
- **Atomic Transfer:** possibilità di raggruppamento di più transazioni in un unico blocco al fine di confermare contemporaneamente (ossia atomicamente) transazioni reciproche di scambio
- **Algorand Smart Contract:** smart contract creati tramite linguaggio TEAL (Transaction Execution Approval Language), un linguaggio Turing complete che supporta loop e subroutine, ma limita la quantità di tempo di esecuzione del contratto utilizzando un algoritmo di valutazione del costo del codice operativo dinamico
  - **Algorand Virtual Machine** (AVM) supporta smart contract stateful, ossia con variabili di stato (locali e globali) con dimensione massima predefinita, similmente a quanto si ha con EVM
- **Algorand State Proof -** una prova crittografica dei cambiamenti di stato che si verificano in un determinato insieme di blocchi
  - Gli State Proof sono strumenti utili per *l'interoperabilità* (certificano l'attività della blockchain anche verso reti esterne) con altre blockchain e permettono l'introduzione di **Light Client**, ossia di partecipanti alla rete Algorand che non necessitano di tutta la catena per svolgere il ruolo di validatore ma possono affidarsi solo sul ramo che parte dall'ultimo State Proof in possesso

Consumo energetico delle blockchain

- Il White House Office of Science and Technology Policy (OSTP) si è espresso sull'impatto ambientale ed energetico delle criptovalute negli Stati Uniti, scoprendo che queste ultime contribuiscono in modo significativo al consumo di energia e alle emissioni di gas serra (GHG).
- Il report, pubblicato l'8 settembre 2022, ha rilevato che le criptovalute utilizzano circa 50 miliardi di chilowattora di energia all'anno negli Stati Uniti, pari al 38% del totale globale.
- Il rapporto afferma: «Il mining di cripto-asset che utilizza la rete elettrica genera emissioni di gas serra - a meno che il mining non utilizzi energia pulita»

- Proof of Work non è una soluzione *green*
- Proof of Stake è una soluzione più sostenibile ma potenzialmente meno sicura
- Pure Proof of Stake è una soluzione sostenibile e contemporaneamente sicura

Consumo energetico delle blockchain – report White House

Summary of the most recent published electricity usage estimates of selected PoW and PoS blockchains (2021-2022)[206]

Crypto-Asset	Market Valuation in August 2022 ($billion)	Consensus Mechanism	Date of Estimate(s)	Global Electricity Usage (TWh/y)			Source
				Best Estimate	Lower Value	Upper Value	
Bitcoin	$389	PoW	8/15/2022	88.6	38.2	179.3	https://ccaf.io/cbeci/index
			8/15/2022	144.9	62.6		https://digiconomist.net/bitcoin-energy-consumption
Ethereum	$185	PoW	8/15/2022	93.9	15.6		https://digiconomist.net/ethereum-energy-consumption
			8/15/2022	22.9	16.5	32.2	https://kylemcdonald.github.io/ethereum-emissions/
Cardano	$15	PoS	9/6/2021		1.4E-04	4.4E-03	https://arxiv.org/abs/2109.03667
			8/8/2021	6.0E-04			https://www.carbon-ratings.com/dl/pos-report-2022
Solana	$11	PoS	10/9/2021	2.0E-03			https://www.carbon-ratings.com/dl/pos-report-2022
Dogecoin	$8	PoW	8/15/2022	3.8			https://digiconomist.net/dogecoin-energy-consumption
Polkadot	$8	PoS	7/5/2021		1.4E-05	4.4E-04	https://arxiv.org/abs/2109.03667
			8/29/2021	7.0E-05			https://www.carbon-ratings.com/dl/pos-report-2022
Avalanche	$6	PoS	10/23/2021	4.9E-04			https://www.carbon-ratings.com/dl/pos-report-2022
Algorand	$2	PoS	8/12/2021		5.4E-05	1.7E-03	https://arxiv.org/abs/2109.03667
			8/17/2021	5.1E-04			https://www.carbon-ratings.com/dl/pos-report-2022
Tezos	$1	PoS	8/12/2021		1.9E-05	5.9E-04	https://arxiv.org/abs/2109.03667
			8/25/2021	1.1E-04			https://www.carbon-ratings.com/dl/pos-report-2022

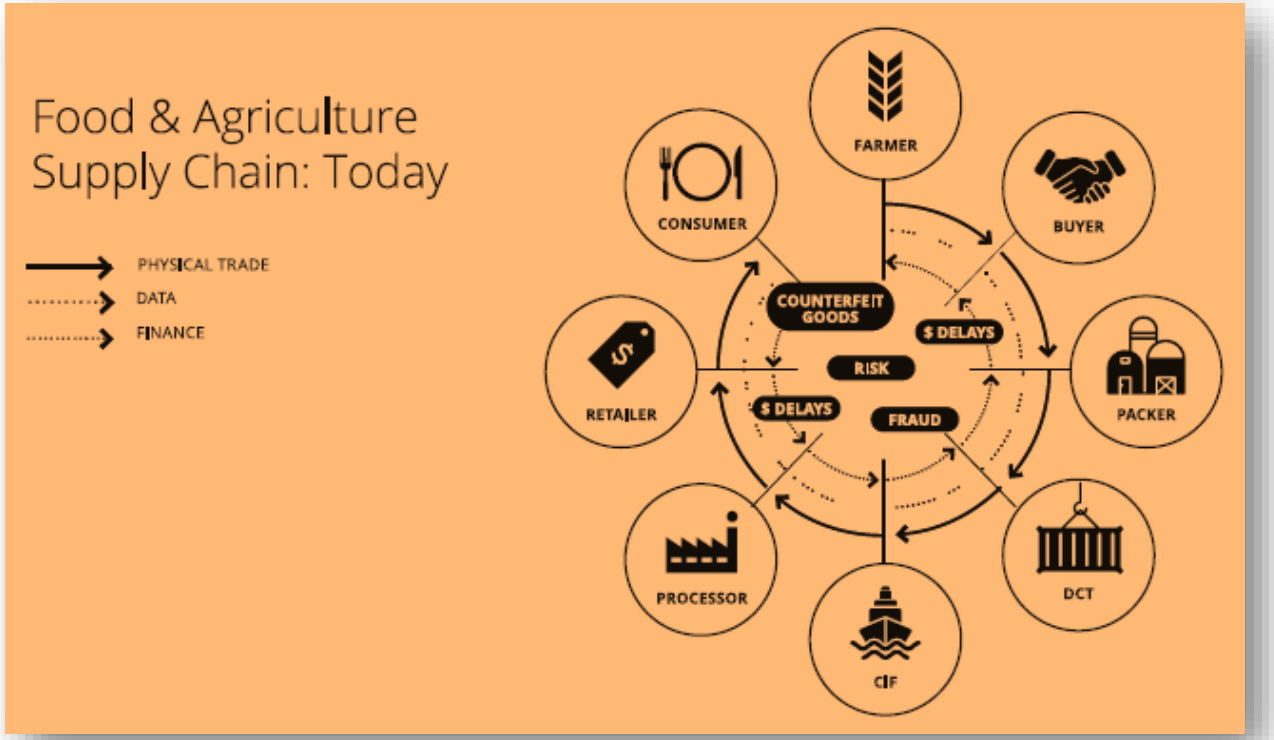
https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf

Use case: supply chain

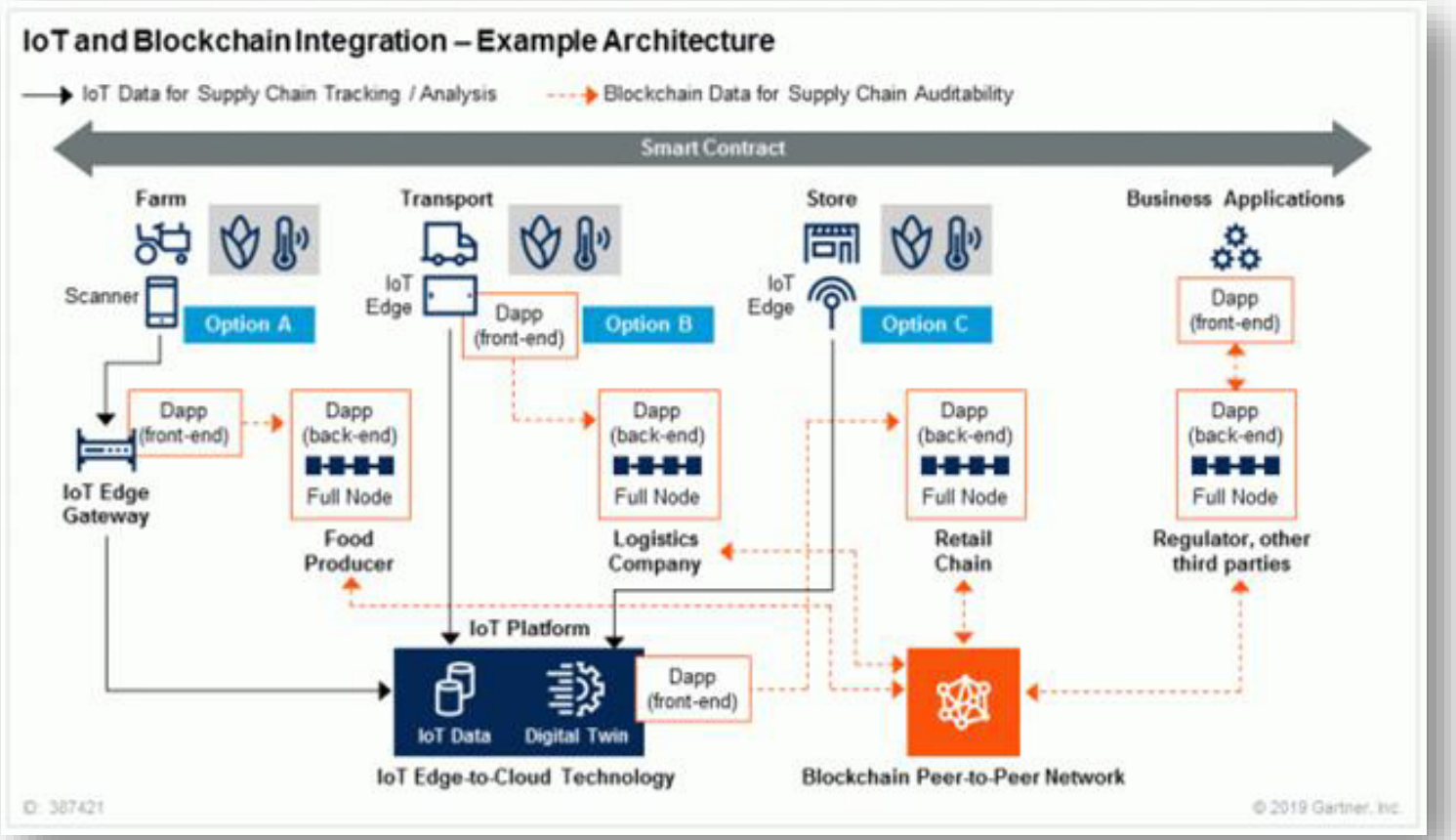
- Uno scenario classico della supply chain, ad esempio nel mondo agricolo, ha come **attori** i coltivatori, i trasportatori, i magazzini di smistamento, i grossisti, i distributori, i rivenditori, i clienti.
- I contratti della supply chain sono complessi perché **coinvolgono più parti**, sono soggetti a **vincoli logistici** e **regolamenti** che possono variare se interessano aree diverse o addirittura perché interessano scambi transfrontalieri.

- *Interoperabilità* – i problemi di semantica e sintassi non mancano mai quando due sistemi diversi devono comunicare
- *Latenza* – dovuta al fatto che gli scambi di merce sono spesso rallentati da burocrazia e carteggi amministrativi
- *Integrità* – bisogna garantire che la filiera del prodotto non possa essere falsificata

La blockchain è lo strumento che risolve tutti i suddetti problemi, tracciando tutti gli scambi informativi e finanziari legati alla catena produttiva



Use case: IoT



- Autenticazione dei device IoT
- Scalabilità del sistema
- Sicurezza applicata ai dati collezionati dai device IoT
- Trasparenza e tracciabilità processamento dati

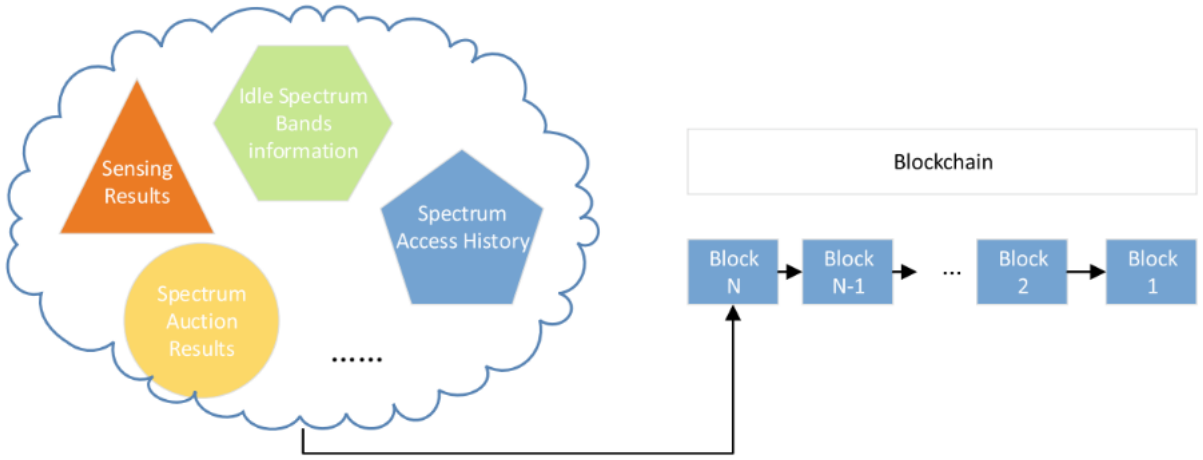
Inoltre…

- Possibilità di interfacciarsi con diverse tecnologie IoT
- Possibilità di implementare sistemi trasparenti di rimunerazione per chi fornisce i dati

Blockchain & Spectrum Management

La blockchain offre nuove opportunità nella gestione dinamica dello spettro radio, ad esempio:

- Può essere utilizzata per i sistemi di asta dello spettro
- Può aiutare a superare le sfide sulla sicurezza o la mancanza di incentivazione per la collaborazione nella gestione dinamica dello spettro
- Può essere utilizzata per registrare in maniera decentralizzata l'uso dello spettro (vedi esperimento ANFR su gestione PMSE tramite blockchain - https://www.anfr.fr/anfr/politique-dinnovation/applications-et-outils)



Esempio di blockchain come sistema di tracciamento delle informazioni usate per lo spectrum management

Ying-Chang Liang, "Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence", Springer 2020

What's next

- L'attuale impegno della Commissione Europea si è focalizzato sulla regolazione dei crypto-asset: lo scorso 20 aprile 2023 è stato approvato dal Consiglio europeo il **Markets in Crypto-Assets Act (MiCA)** per garantire la sicurezza degli investitori ed evitare fenomeni di insolvenza come nel caso FTX.
- Per quanto riguarda l'uso della blockchain nella realizzazione di soluzioni applicative, l'Europa ha costituito **la European Blockchain Services Infrastructure (EBSI)**, nata nel 2018 quando 29 paesi (tutti gli stati membri dell'UE, Norvegia e Liechtenstein) e la Commissione UE hanno unito le forze per creare la **European Blockchain Partnership (EBP)**.
- La visione di EBP è quella di sfruttare la blockchain per creare servizi transfrontalieri per pubbliche amministrazioni, imprese, cittadini e i loro ecosistemi per verificare le informazioni e rendere i servizi affidabili.
- Tra i progetti più ambiziosi di EBSI c'è lo sviluppo di un modello di **Verifiable Credentials** finalizzate alla costituzione di un *European Digital Identity Wallet*, come anticipato dal nuovo regolamento eIDAS.
- In Italia, il riconoscimento giuridico della *Distributed Ledger Technology* e quindi delle *blockchain* lo si deve al *Decreto Semplificazione 2019* (*D.L 14/12/2018 n.135 art. 8ter*); nonostante sia riconosciuta l'efficacia della tecnologia, rimangono tuttavia ancora da definire linee guida per la realizzazione di servizi basati su di essa e per la creazione di smart contract.

Grazie per l'attenzione!

Domande?

Albenzio Cirillo
acirillo@fub.it