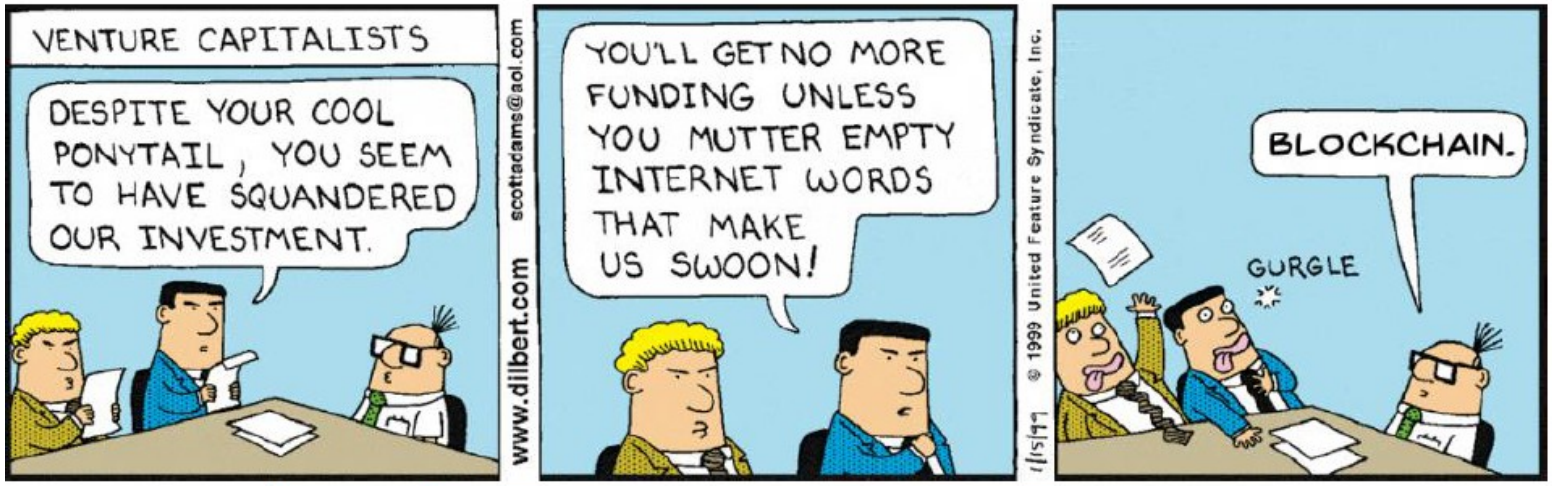
BLOCKCHAIN: OLTRE LE CRYPTOCURRENCIES

Laura Ricci
Dipartimento di Informatica
Università degli Studi di Pisa
online, 10 dicembre 2020

BLOCKCHAIN OLTRE L'HYPE

- solo una buzzword?
  - assolutamente no: una tecnologia veramente innovativa e disruptive
- ma...serve più consapevolezza, più formazione, più ricerca
- coinvolgere computer scientists, giuristi, economisti su aspetti diversi
  - formazione in diverse lauree magistrali
  - contatti con altri gruppi: Sant'Anna, Giurisprudenza, Cambridge
  - progetti europei e nazionali

BLOCKCHAIN: CAVALCHIAMO L'HYPE!

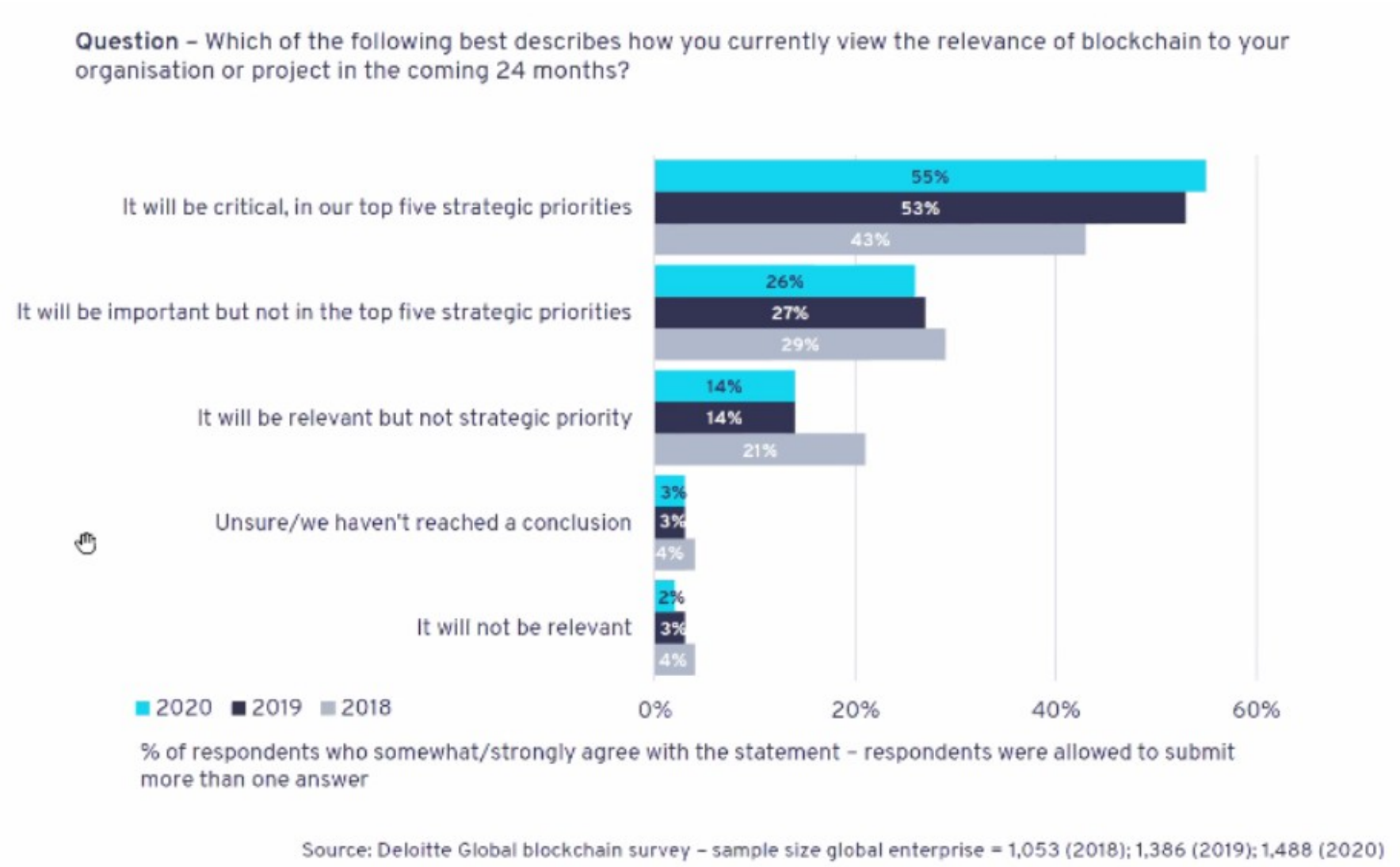


MENU CNBC MARKETS BUSINESS NEWS INVESTING TECH

Salaries for blockchain engineers are skyrocketing, now on par with AI experts

- Blockchain engineers are making between $150,000 and $175,000 in annual salaries on average.
- Blockchain engineers are the top paid roles in software development, on par with specialists focused on artificial intelligence.
- Demand for blockchain engineers has increased by 400 percent since late 2017 on Hired, a firm that helps clients recruit tech candidates.

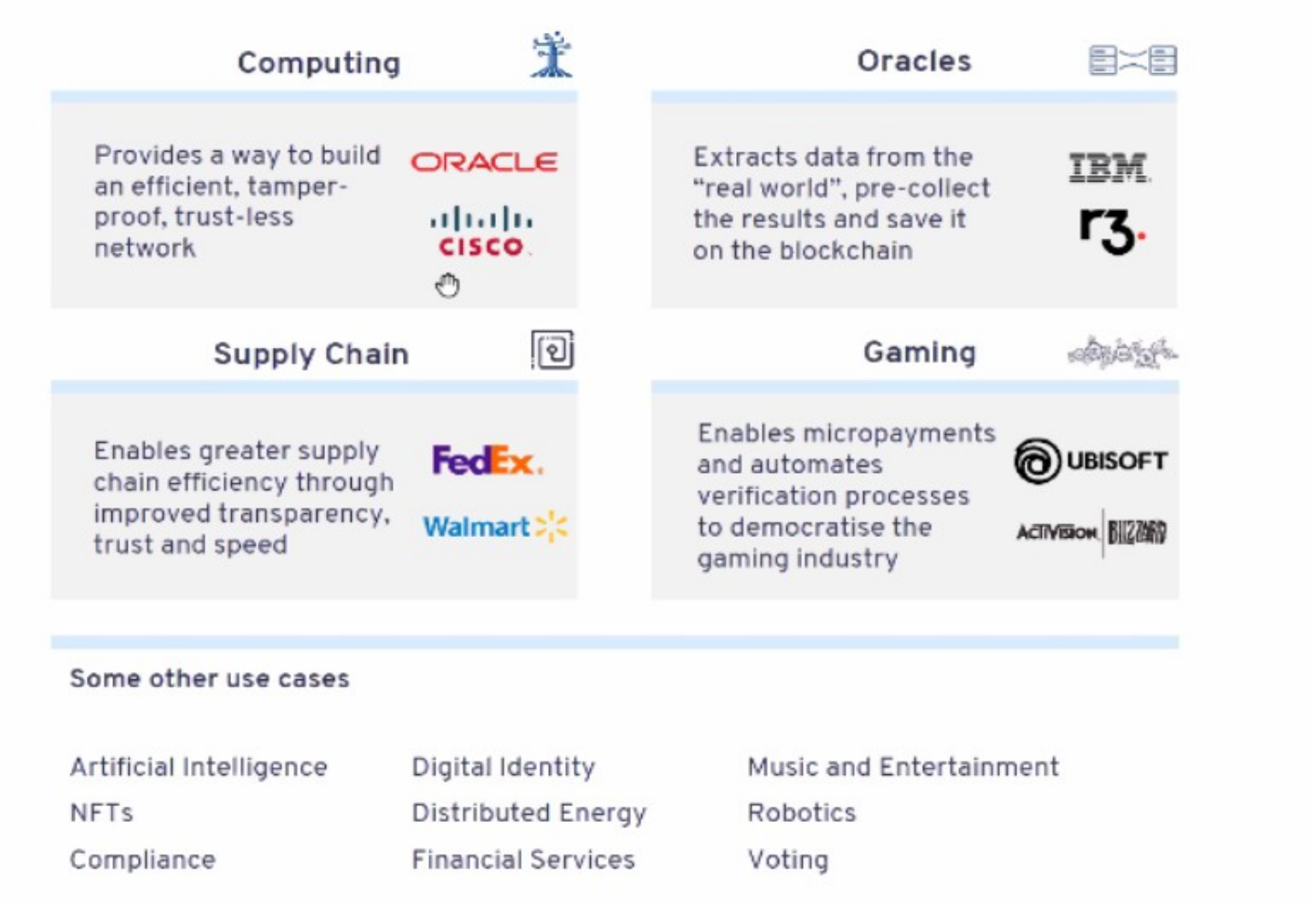
BLOCKCHAIN: MA E' VERAMENTE UN L'HYPE?



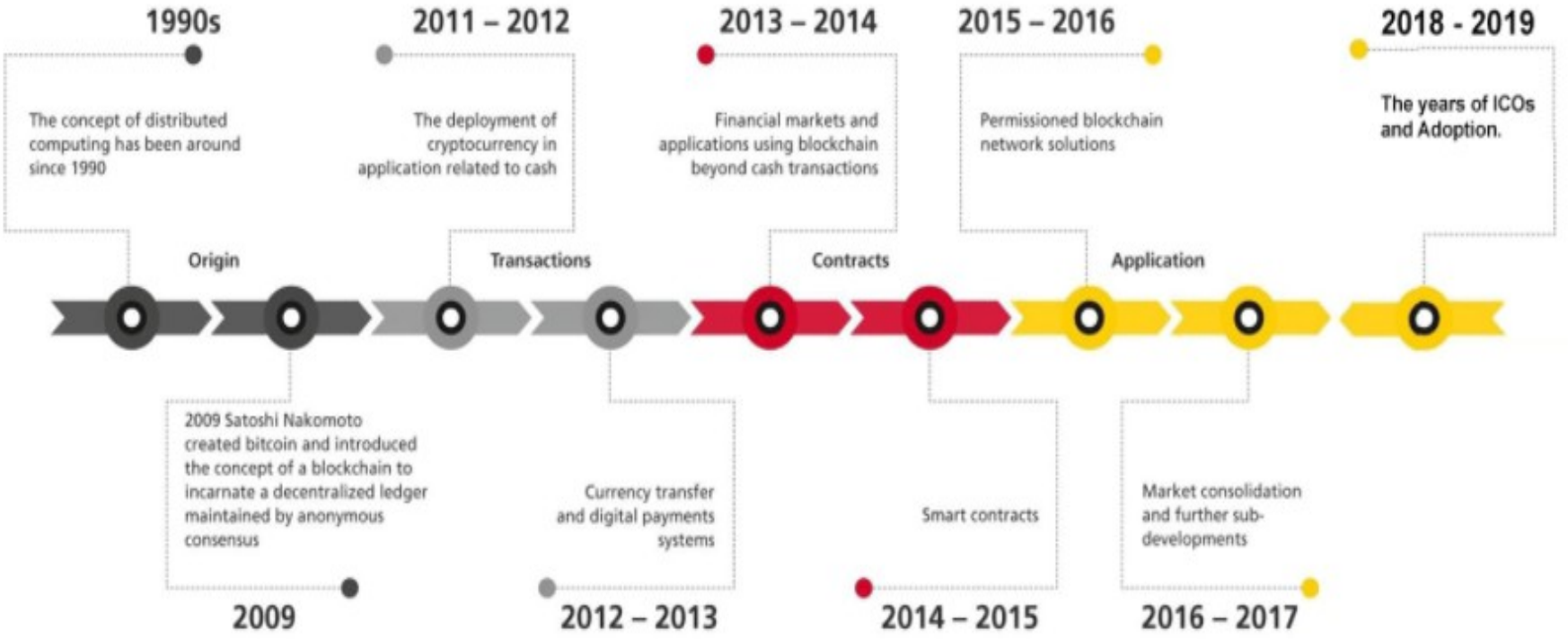
ALCUNI INVESTIMENTI IMPORTANTI

Portfolio Company	Company Information	Lead Investor
ØRIGIN	Protocol for building cheaper decentralised Uber and Airbnb	PANTERA
DFINITY	World computer network that is powerful enough to host business applications at scale to rival Amazon Web Services	ANDREESSEN HOROWITZ
Algorand™	Blockchain infrastructure that enables frictionless finance	USV
Hedera Hashgraph	Decentralised public network governed by the world's leading organisations (Google, IBM, Nomura, DLA Piper, Boeing, etc.)	DIGITAL CURRENCY GROUP
BORDERLESS CAPITAL.	A venture capital fund investing in category-leading businesses leveraging blockchain technology	arrington XRP CAPITAL

ALCUNI INVESTIMENTI IMPORTANTI



DIECI ANNI DI UNA TECNOLOGIA "DISRUPTIVE"



"LA MADRE DI TUTTE LE BLOCKCHAIN": BITCOIN

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

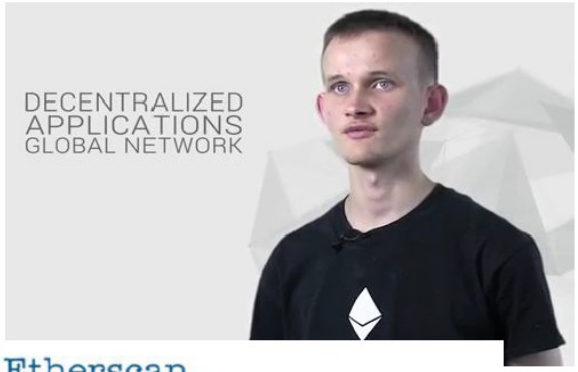
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of

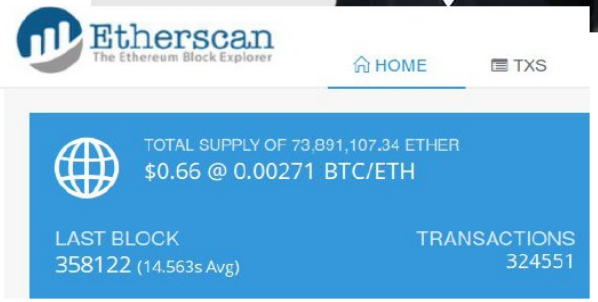
```
bitcoin-0.1.0.rar
bitcoin-0.1.0.tgz
```

Paper published in October 2008: 12 years of Bitcoin!

E L'ALTRA SUPESTAR.... ETHEREUM E BUTLERIN

- crowdfunding ~$20M in un mese
- idea di generalizzare la tecnologia delle criptomonete
- Vitalik Butlerin: 2014-2015

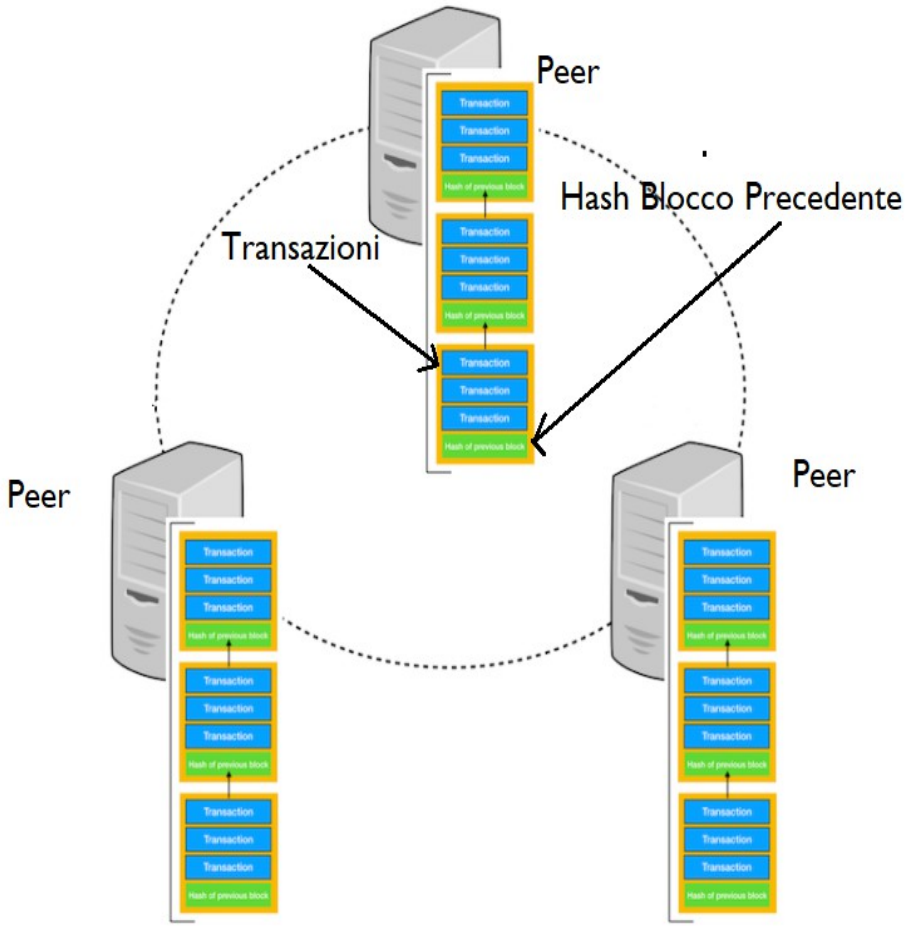




- blockchain programmabile con un linguaggio Turing-completo
- smart contracts
  - Solidity
  - Serpent
- eseguiti da tutti i nodi: consenso sul risultato della computazione

BLOCKCHAIN IN BREVE

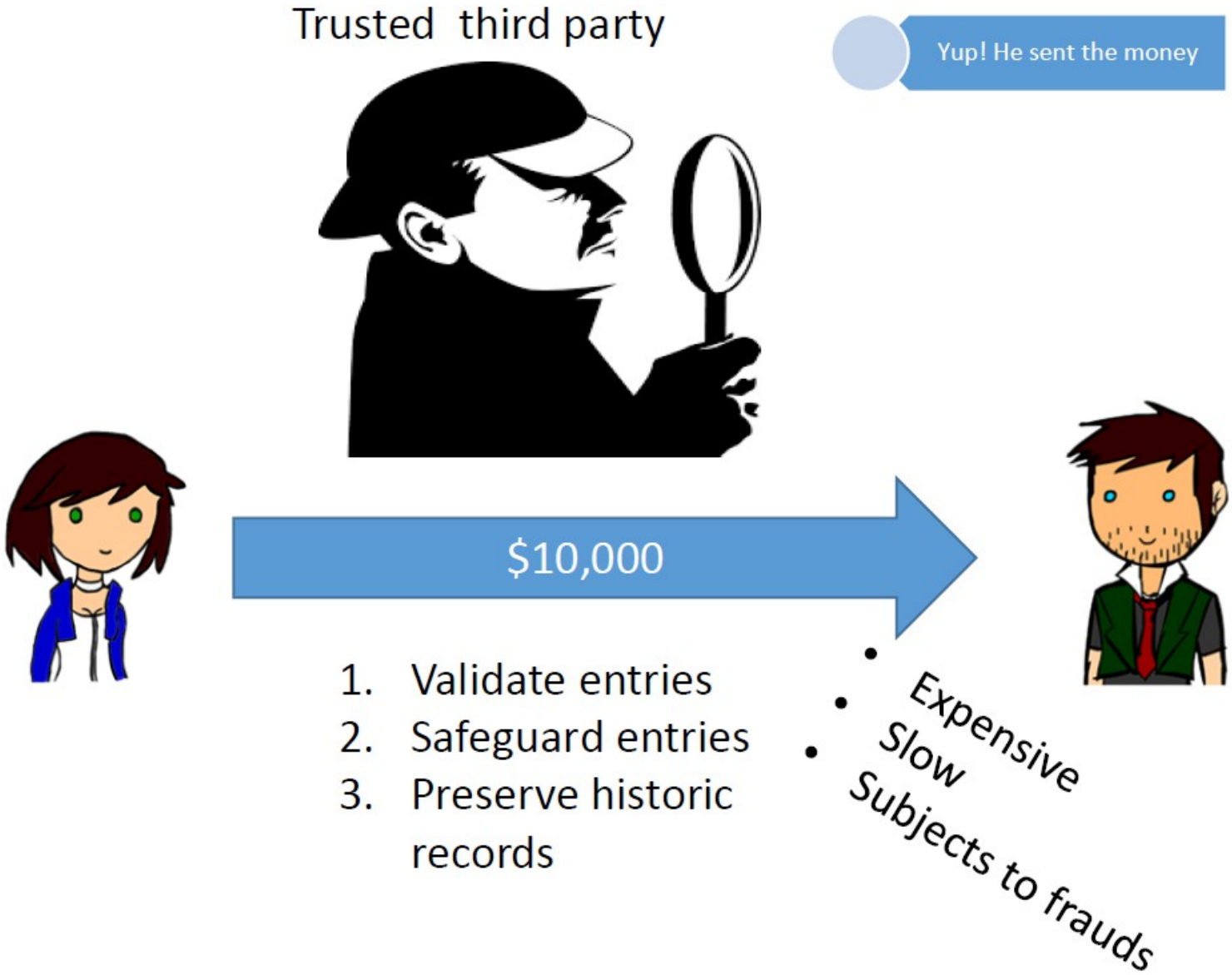
- database distribuito e replicato sui nodi di un sistema peer to peer (P2P)
  - un insieme di blocchi collegati mediante puntatori hash
  - in ogni blocco è presente l'hash blocco precedente
  - ogni peer possiede una copia consistente dell'intero database
- operazioni
  - append only: accodare progressivamente registrazioni organizzate in blocchi
  - leggere il contenuto di una qualsiasi registrazione



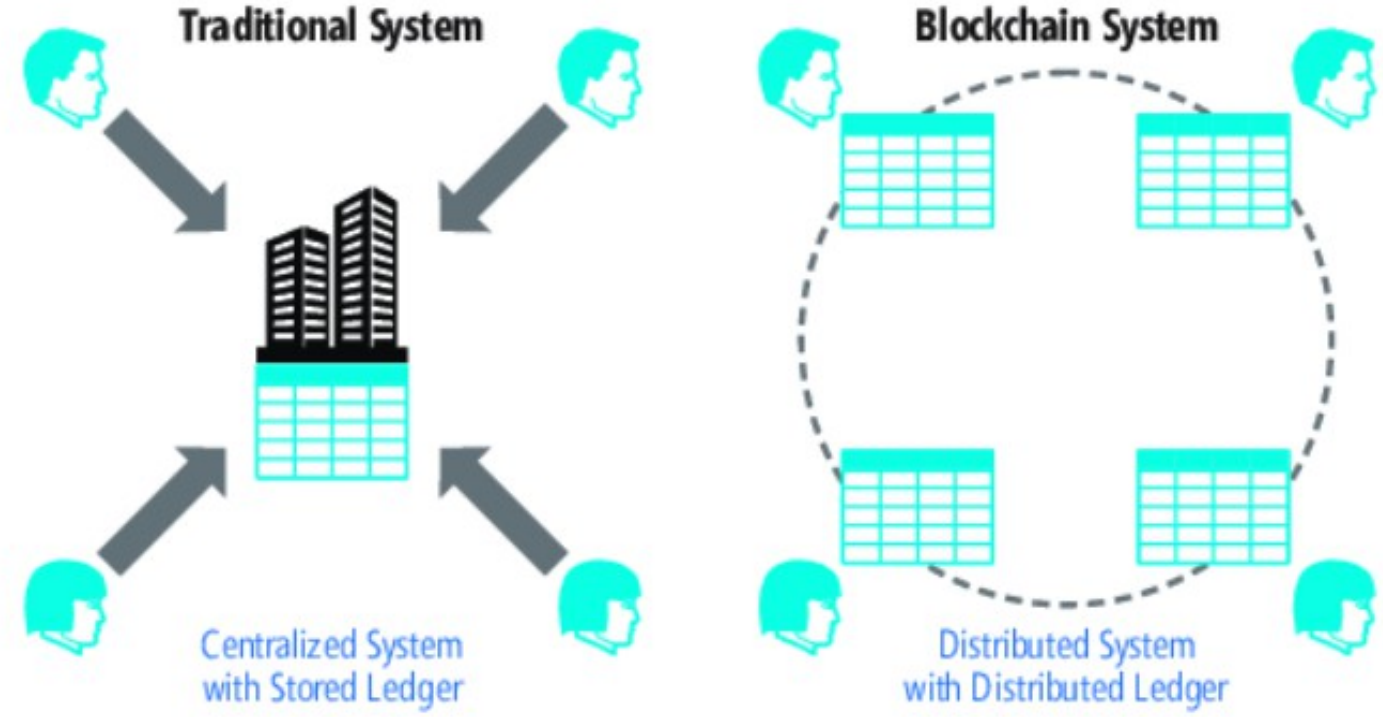
ALCUNE PROPRIETA' IMPORTANTI

- distribuzione del controllo
- tamper freeness
  - nessuno può modificare una registazione scritta in precedenza, e neppure aggiungere una registrazione tra due già esistenti
- trasparenza
  - "tutti" possono verificare la correttezza delle transazione e leggerne il contenuto
  - ma cosa metto su blockchain? compromesso privacy-trasparenza...
- consistenza
  - "tutti i nodi della rete" possiedono esattamente la stessa copia della blockchain
  - un blocco viene aggiunto alla blockchain solo quando tutti i nodi hanno acconsentito al suo inserimento nella blockchain
  - algoritmi distribuiti di consistenza

IDEA DI BASE: ASSENZA DI TERZE PARTI FIDATE



….SUPERARE COSI' IL PARADIGMA CLIENT SERVER

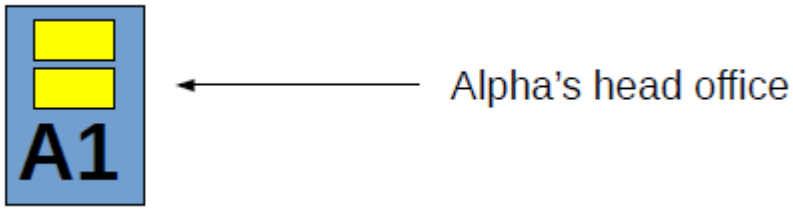


MA COSA METTIAMO SULLA BLOCKCHAIN?

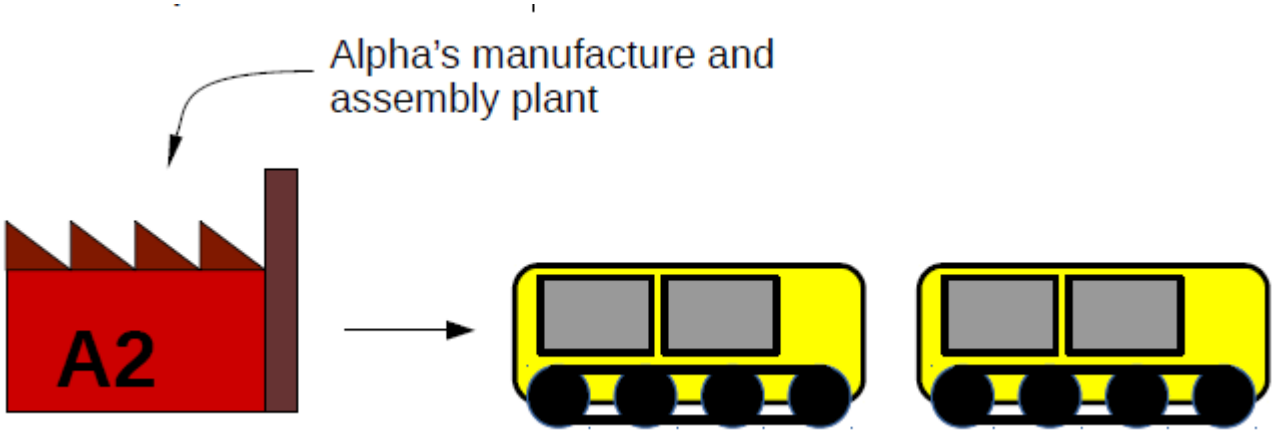
- in generale, transazioni
- trasferimenti di cryptomoneta (Bitcoin, Ethereum,...)
- ma non solo!
  - rilevazione da sensori IoT, E.G.,...
  - proprietà intellettuale/fruzione di un contenuto audio/video
  - concessione del diritto ad accedere a dati sensibili (dati medici,.....)
  - transazioni finanziarie
  - manutenzione asset
  - tracciamento di supply chain (e.g.: diamanti,....)
  - in generale, processi a cui partecipano più entità indipendenti in un ambiente trustless

OLTRE LE CRIPTOCURRENCIES: LA ALPHA CHAIN

- la Alpha company progetta e supervisiona la costruzione di macchinari per l'industria pesante
- A1 è la struttura dirigenziale della Alpha company

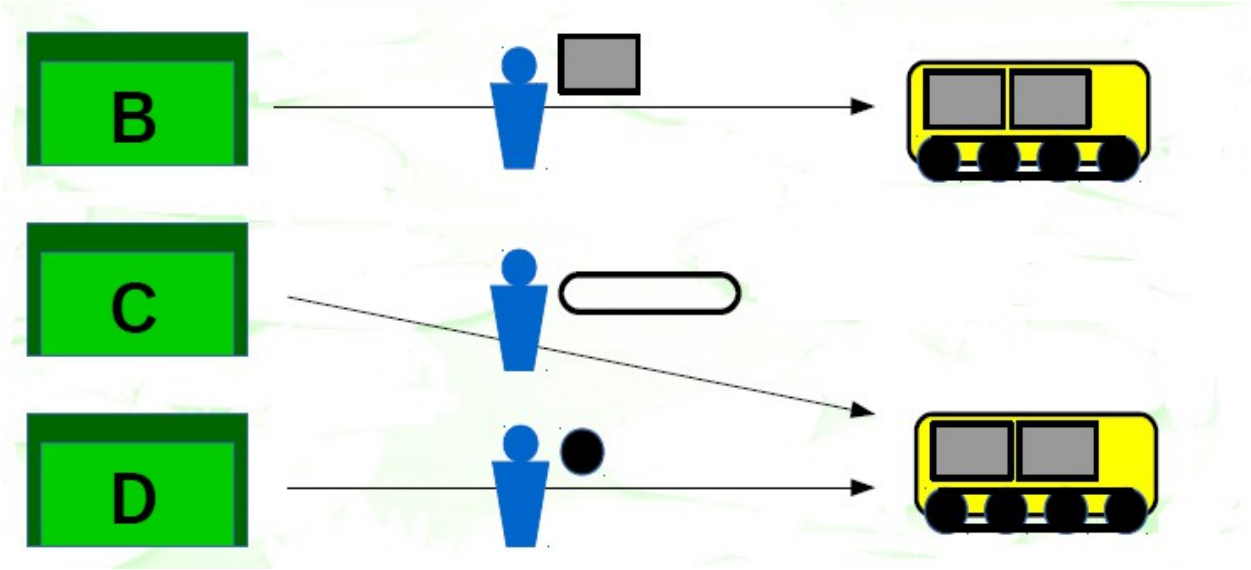


- le componenti dei macchinari pesanti sono prodotte ed assemblate in una delle fabbriche della Alpha, A2



OLTRE LE CRIPTOCURRENCIES: LA ALPHA CHAIN

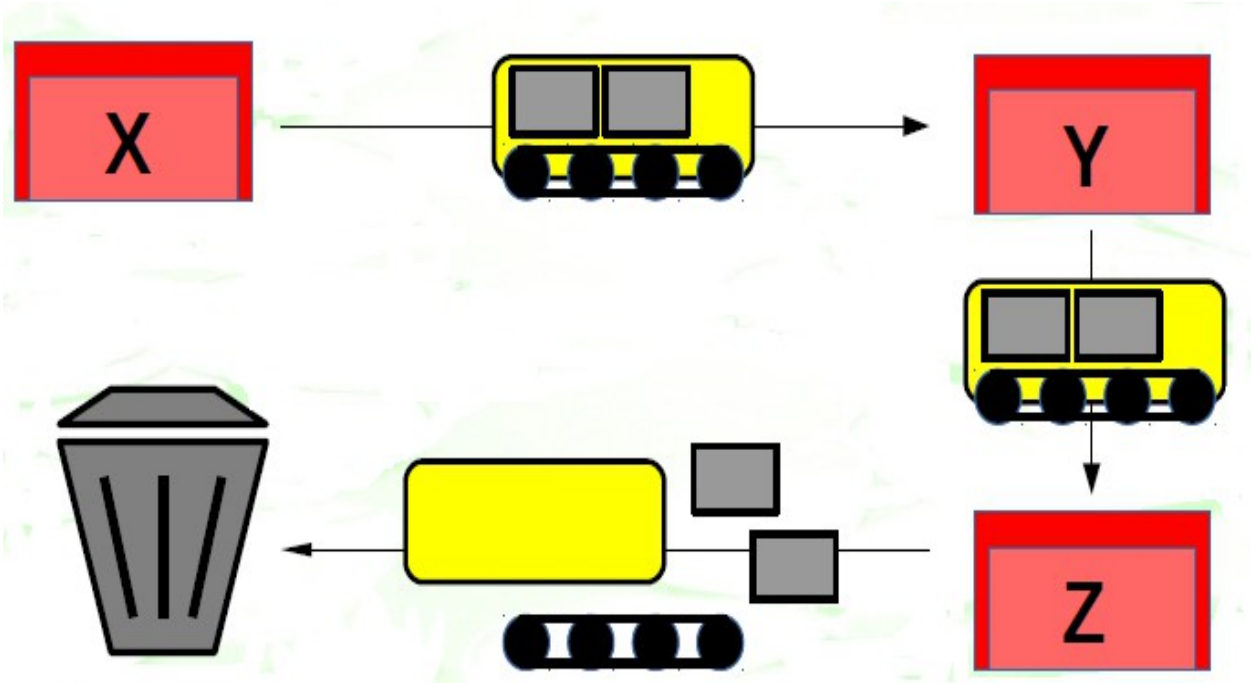
- i macchinari vengono poi inviati ai clienti, che li usano pesantemente.
- i macchinari devono essere revisionati periodicamente per essere conformi alla legislazione locale riguardante le regole di sicurezza



- Alpha stipula contratti di gestione con terze parti autorizzate, che si avvalgono di personale certificato per la revisione dei pezzi.

OLTRE LE CRIPTOCURRENCIES: LA ALPHA CHAIN

- i macchinari possono essere venduti da una società ad un'altra ed è importante tenere traccia della loro provenienza e storia
- alla fine del ciclo di vita i macchinari vengono smantellati e lo smaltimento dei rifiuti è soggetto alla legislazione locale



ALPHA CHAIN: PERCHE' UNA BLOCKCHAIN

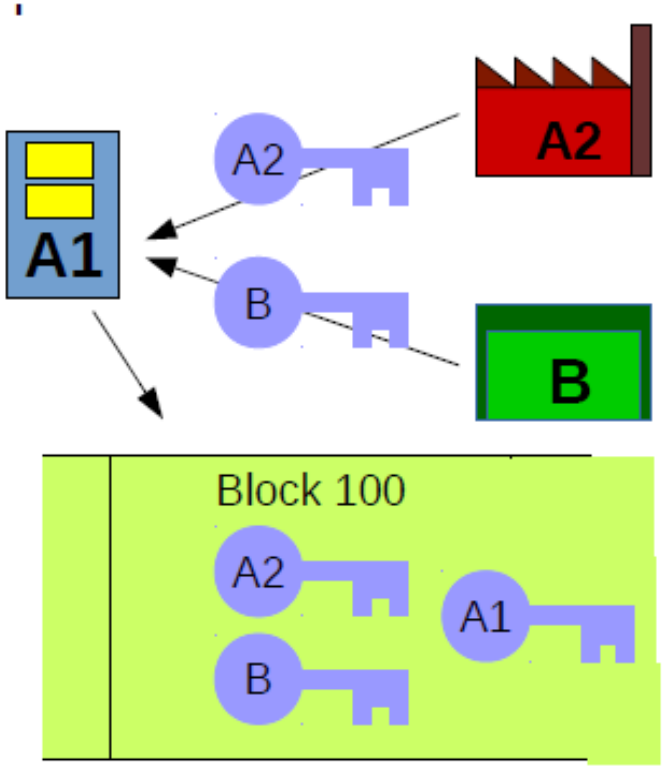
- la blockchain è una struttura distribuita:
  - nodi appartenenti ad organizzazioni diverse (Società Alpha, terze parti, smaltitori) possidono una copia della blockchain
  - ma... non esiste un rapporto di fiducia tra di essi
- è una struttura affidabile (trusted) e garantisce
  - tamper proofness: se un blocco di transazioni è registrato sulla blockchain è "sigillato" e non può più essere modificato
  - consistenza delle copie
    - garantita da algoritmi di consenso: se la maggioranza dei nodi è onesta, l'affidabilità della blockchain è garantita
  - *tecnologia trusted in un ambiente trustless*
- è una struttura pubblica
  - auditing i partecipanti possono analizzare la blockchain e tracciare gli eventi

ALPHA CHAIN: PERCHE' UNA BLOCKCHAIN

- supporta gli "smart contracts"
  - programmi eseguiti da tutti i nodi
  - consenso sui risultati della esecuzione del contratto
  - integrati con dispositivi IoT possono attivare autonomamente richiesta di assistenza quando il limite d'uso è raggiunto
    - quando un macchinario della Alpha ha bisogno di manutenzione, invio automatico di un messaggio all'assistenza
  - possono mantenere la storia delle componenti, dalla creazione agli interventi, alla dismissione

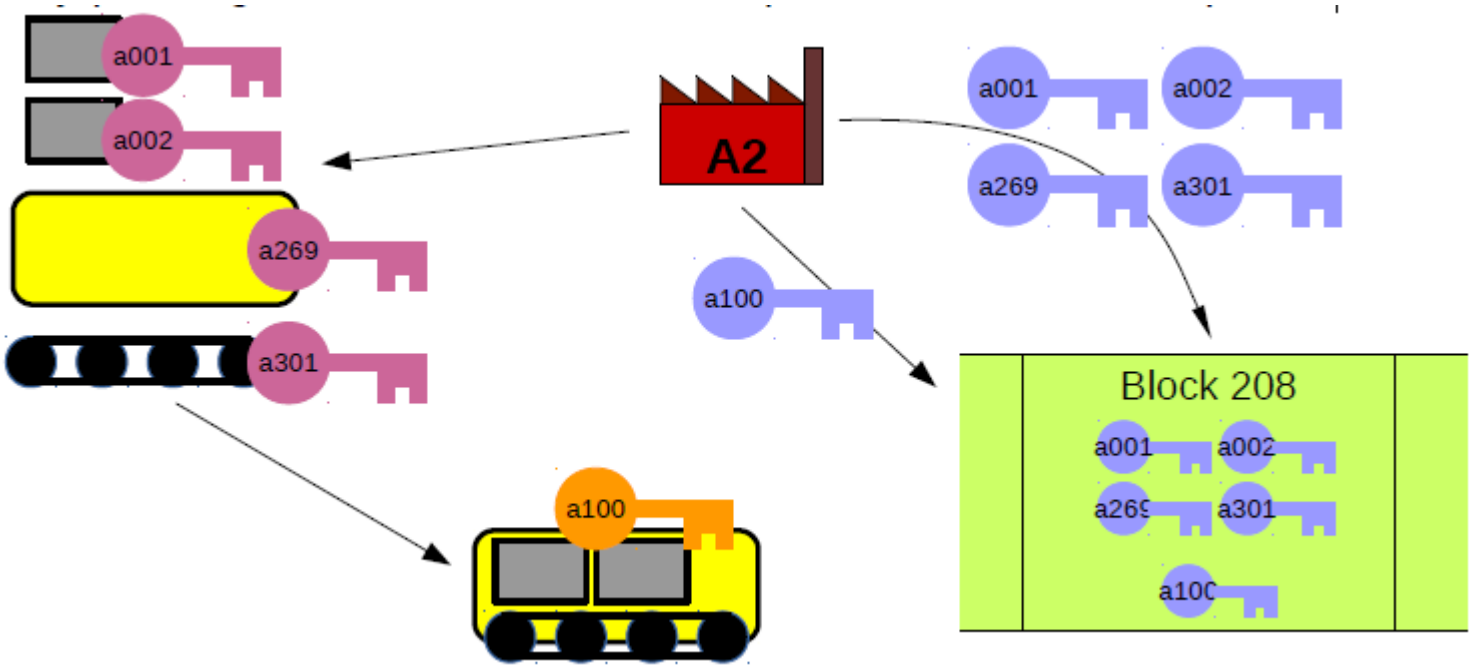
LA ALPHA CHAIN

- la società Alpha attiva una blockchain "permissioned"
  - crea il "blocco genesi"
- gli attori della supply-chain registrano le loro chiavi pubbliche sulla blockchain
  - struttura dirigenziale, fabbrica, terze parti
  - Identità distribuita, non esiste una terza parte che certifica



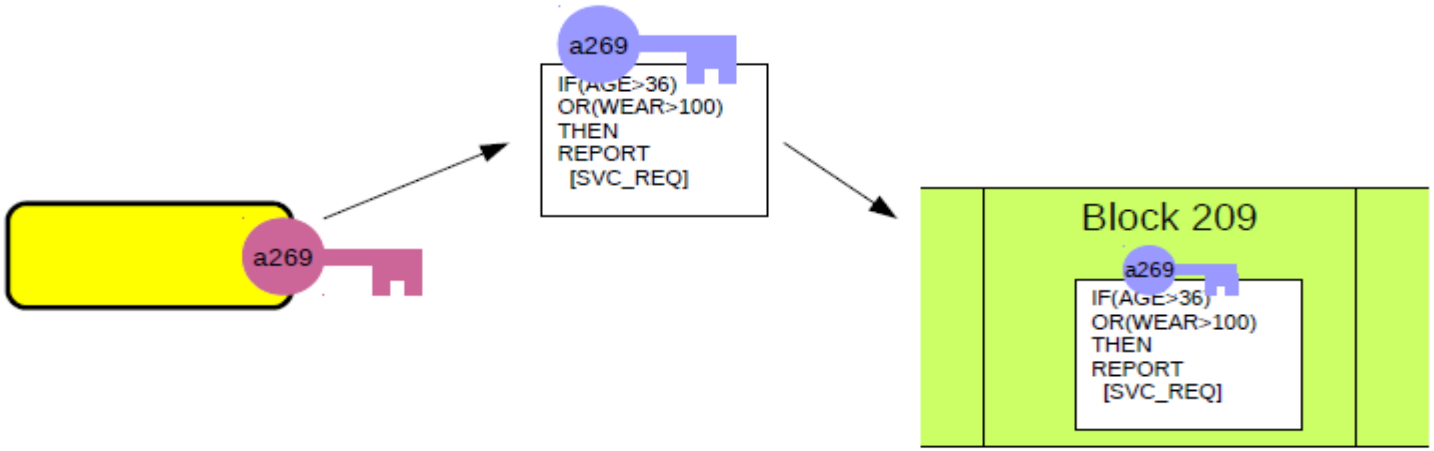
LA ALPHA CHAIN

- la fabbrica A2, crea le componenti
  - per ogni componente coppia chiave pubblica/chiave private
  - chiave pubblica delle componenti sulla blockchain
  - le componenti vengono assemblate: anche per il prodotto finito una coppia chiave pubblica/privata



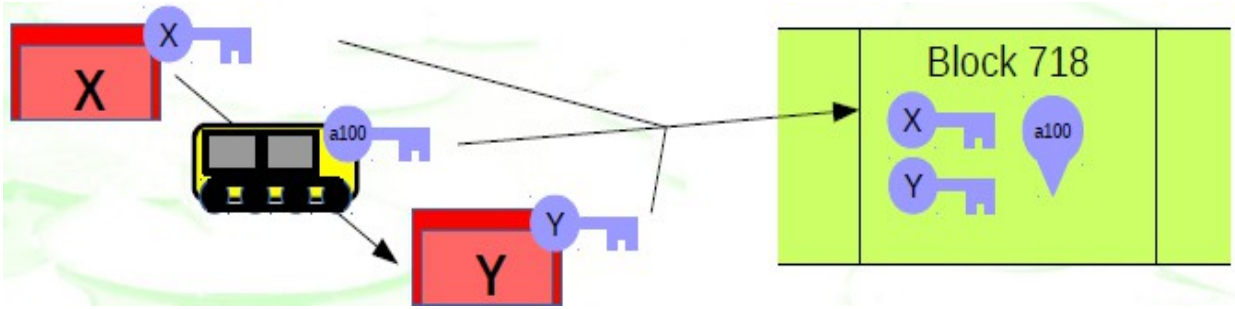
LA ALPHA CHAIN

- uno smart contract per ogni componente
- può essere attivato da un dispositivo IoT "montato" su una componente
- attiva la richiesta di servizio alla società di manutenzione, se la componente va riparata oppure un alert per dismettere il componente, se raggiunto limite di uso

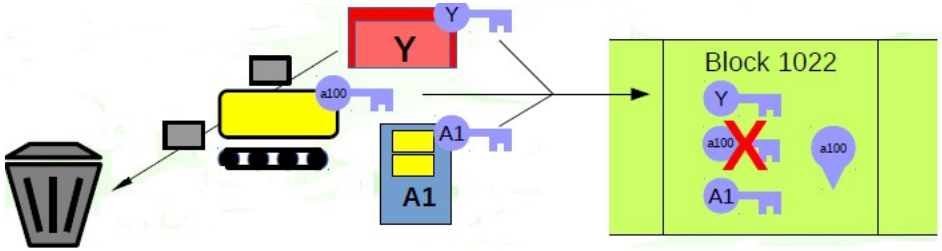


LA ALPHA CHAIN

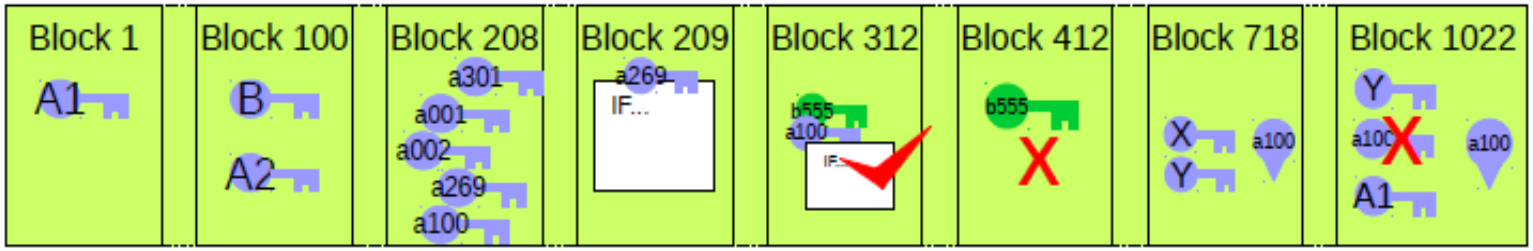
- la società X vende il macchinario alla società Y
  - modifica di proprietà della macchina registrata su blockchain
  - fornisce prova di proprietà per processi di auditing



- alla fine del ciclo di vita, il macchinario viene dismesso
  - l'evento è registrato sulla blockchain, firmato dalla società Alpha
  - permette processo di auditing da parte delle autorità per verificare che la legge sui requisiti ambientali è stata rispettata



LA ALPHA CHAIN



alla fine del processo, la blockchain mantiene un ledger che memorizza in modo permanente e trasparente

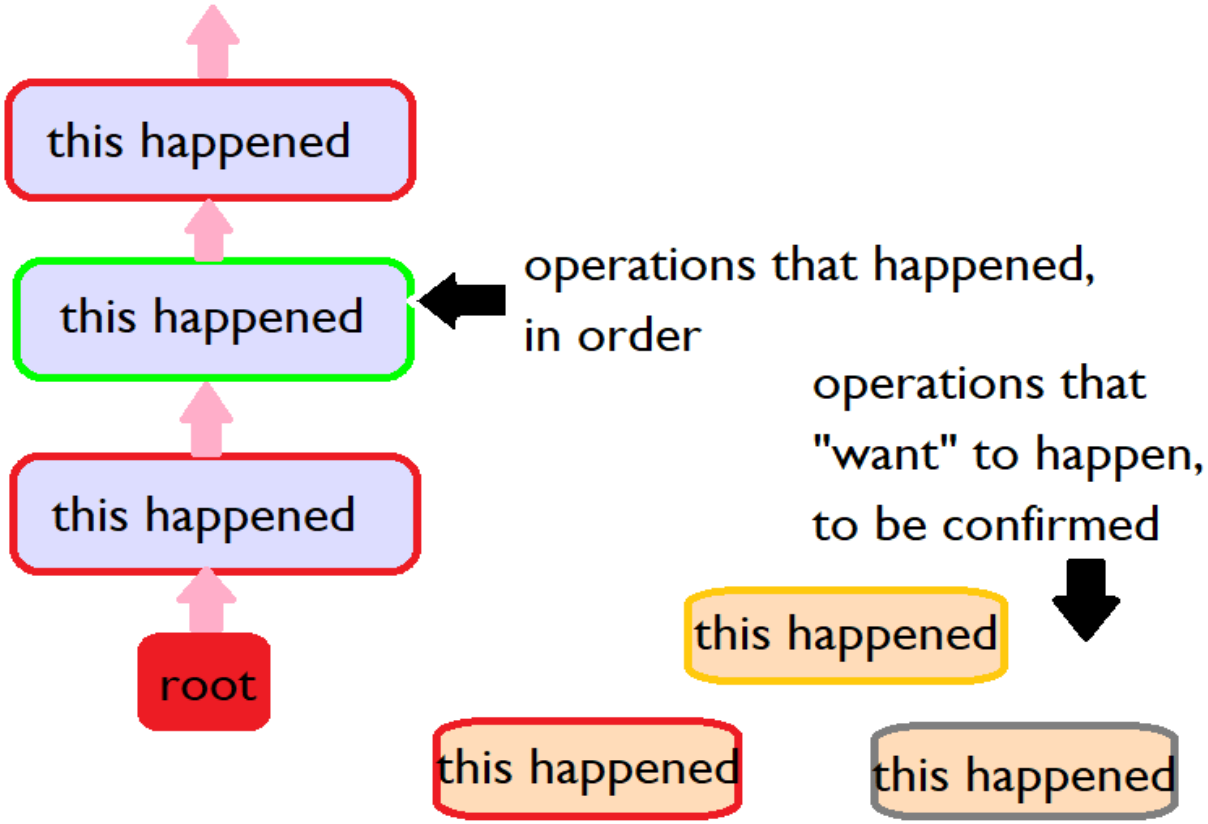
- i partecipanti
- le componenti
- le manutenzioni
- i trasferimenti di proprietà
- lo smantellamento finale

le registrazioni non possono essere eliminate o modificate

- trasparenza: nessun server centralizzato di cui fidarsi
- garanzia di consistenza delle versioni e tamper freeness

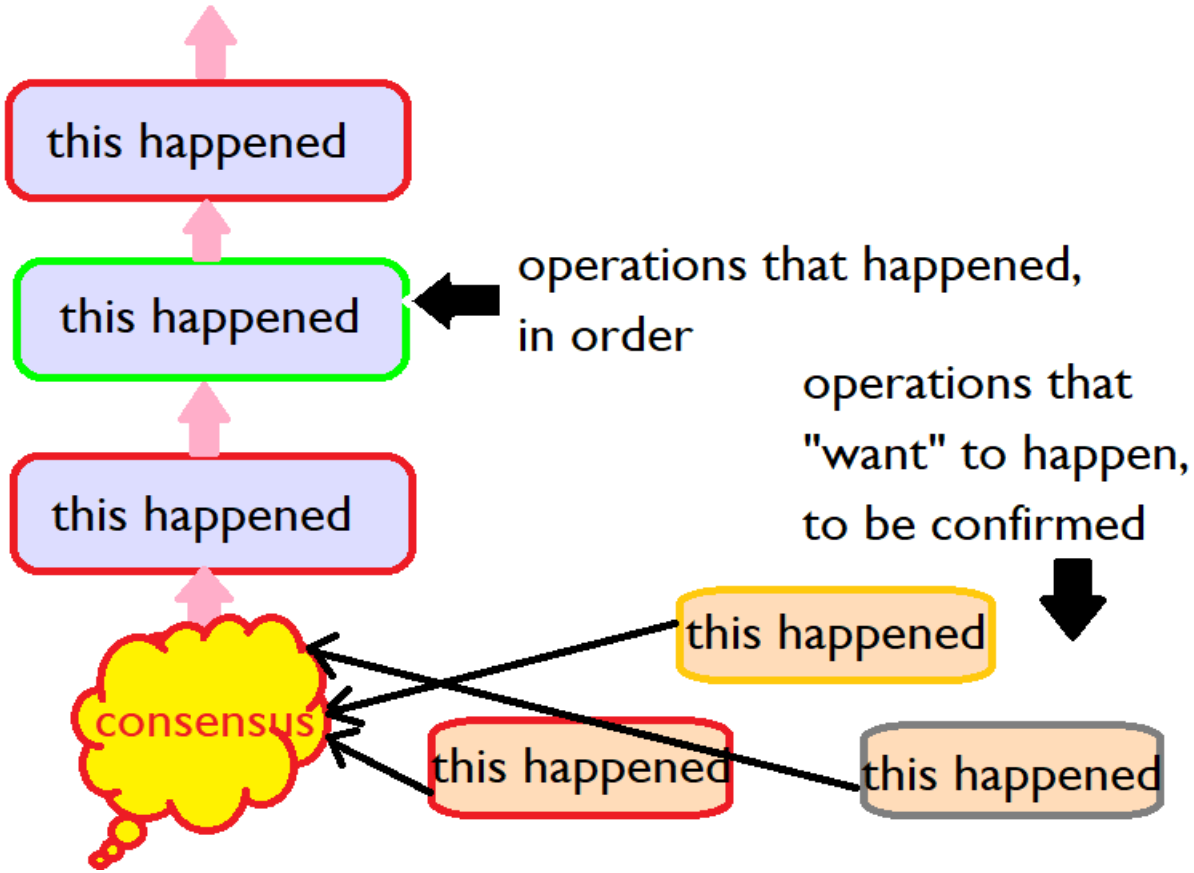
UN PO' DI TECNOLOGIA...

- un registro condiviso
  - se organizzato in blocchi blockchain
  - ma altre strutture sono possibili, ad esempio, strutture a grafo



semplifichiamo: una operazione per ogni blocco

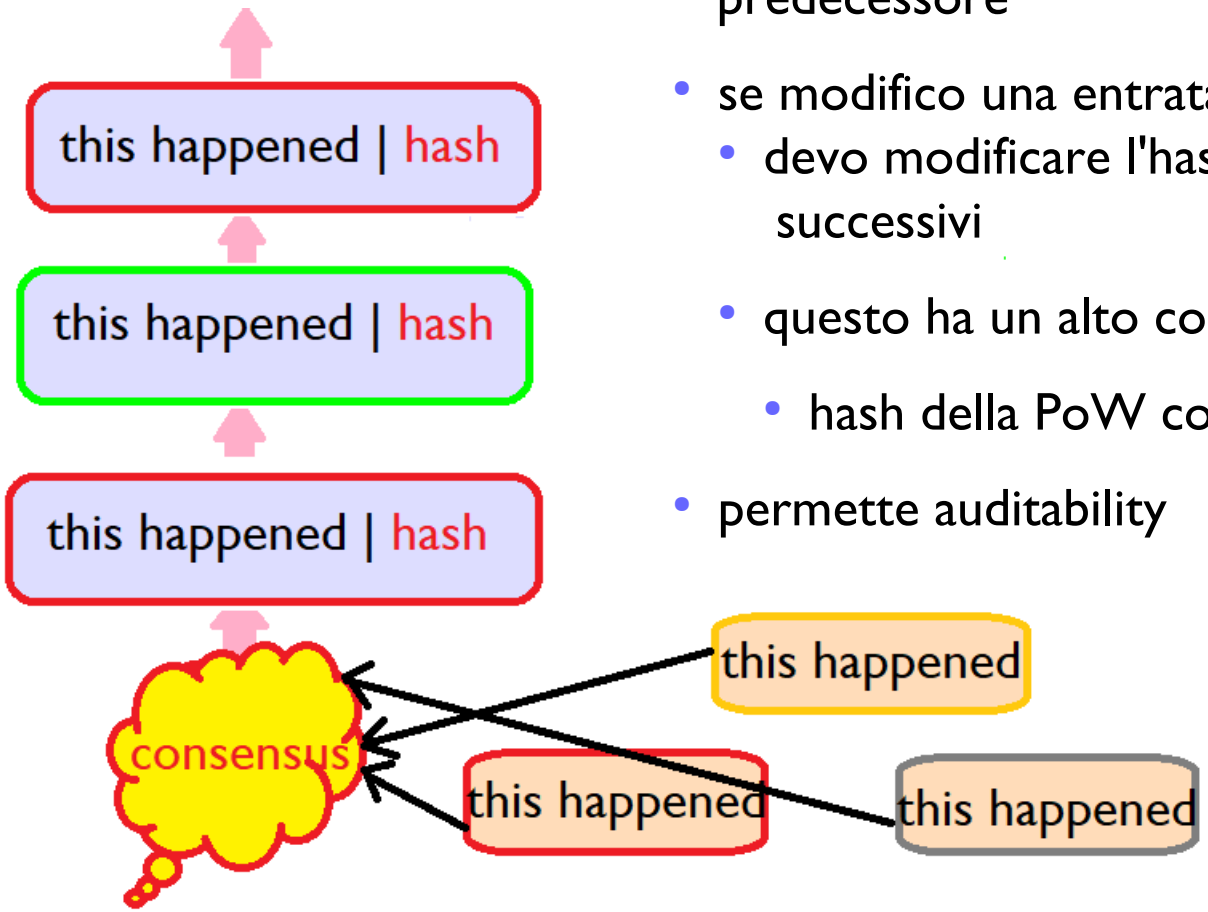
AGGIUNGERE ELEMENTI ALLA BLOCKCHAIN



il consenso è il meccanismo tramite il quale si decide

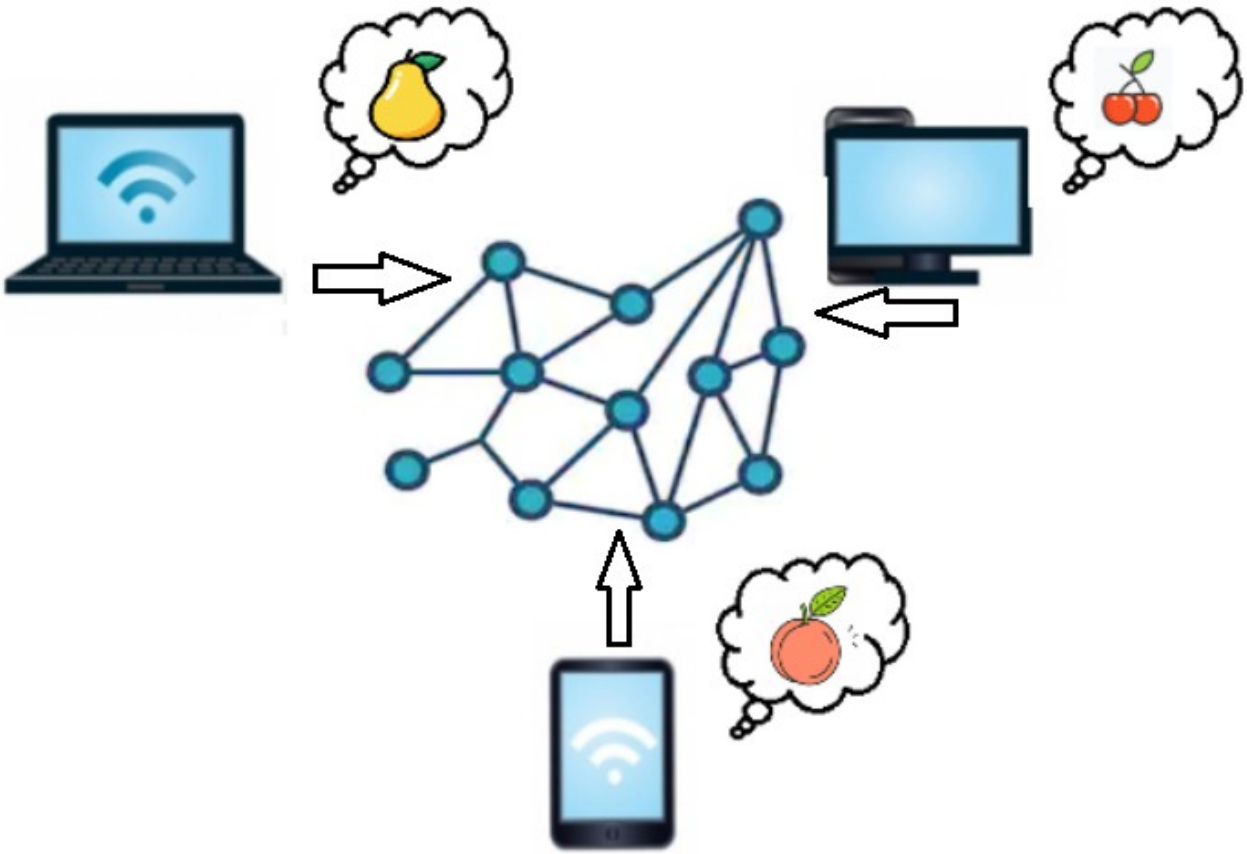
- chi decide quale transazione verrà aggiunta alla blockchain
- quale transazione, tra quelle validate, verrà aggiunta alla blockchain

TAMPER FREENESS



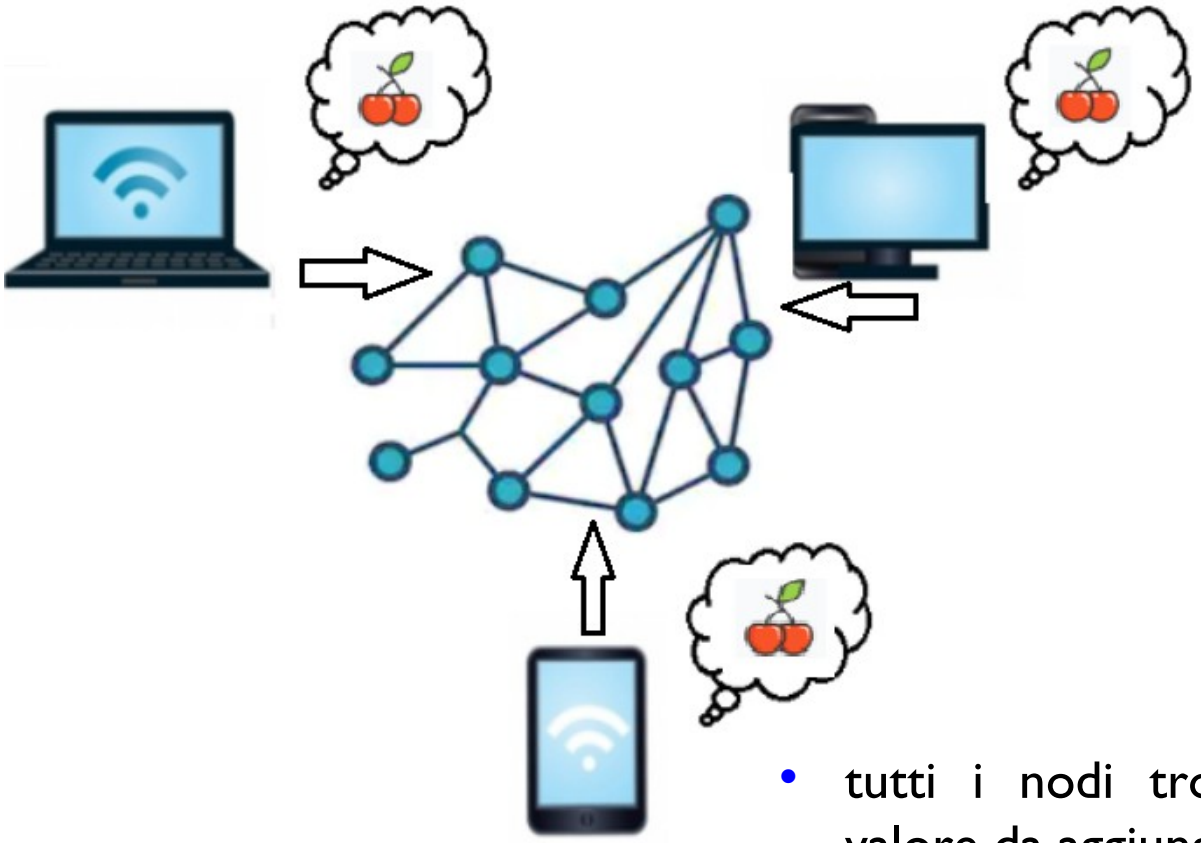
- calcolo dell'hash di ogni blocco
- memorizza in ogni entrata l'hash del blocco predecessore
- se modifico una entrata
  - devo modificare l'hash di tutti I blocchi successivi
  - questo ha un alto costo computazionale
    - hash della PoW con il contenuto del blocco
- permette auditability

COSA E' IL CONSENSO?



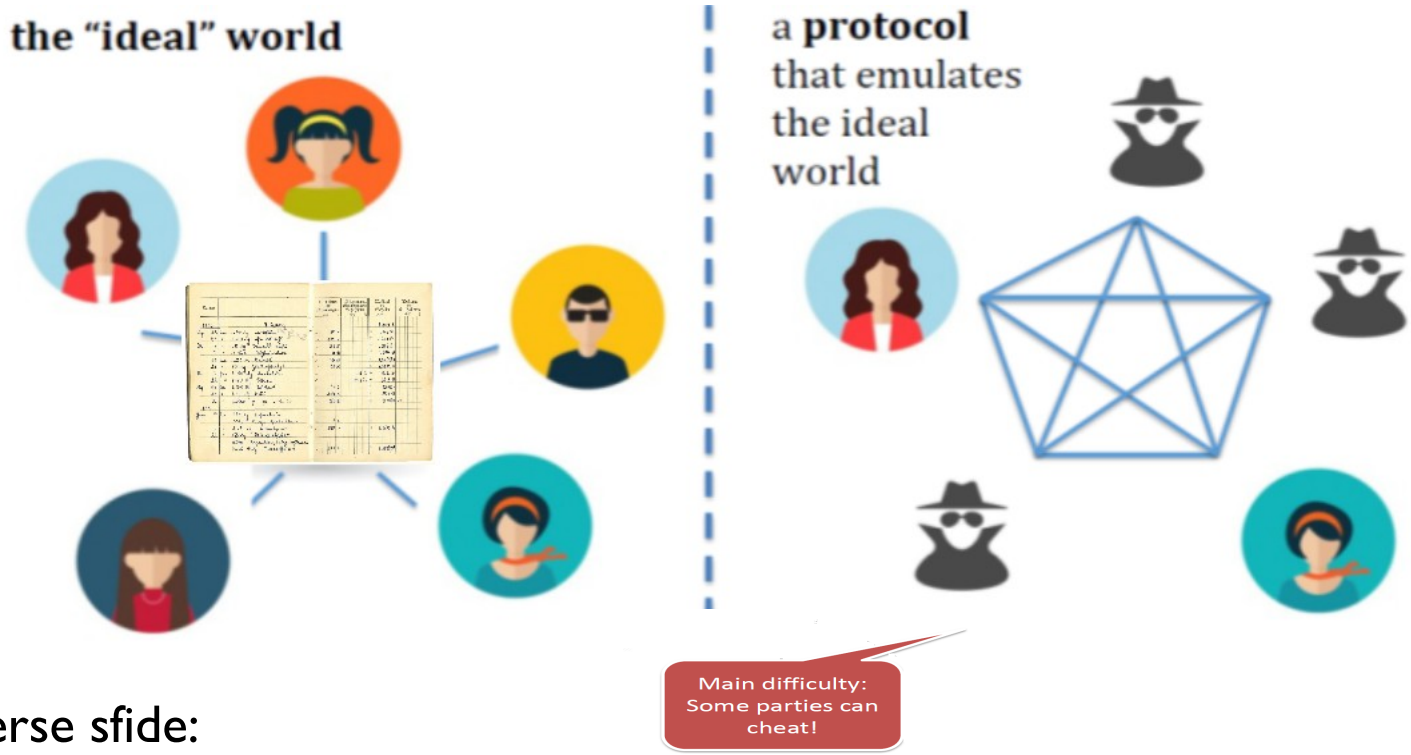
Ogni nodo presenta agli altri un elemento da agguingere alla blockchain

COSA E' IL CONSENSO?



- tutti i nodi trovano un accordo tra il valore da aggiungere alla blockchain
- attenzione: nodi maliziosi o guasti possono esistere!

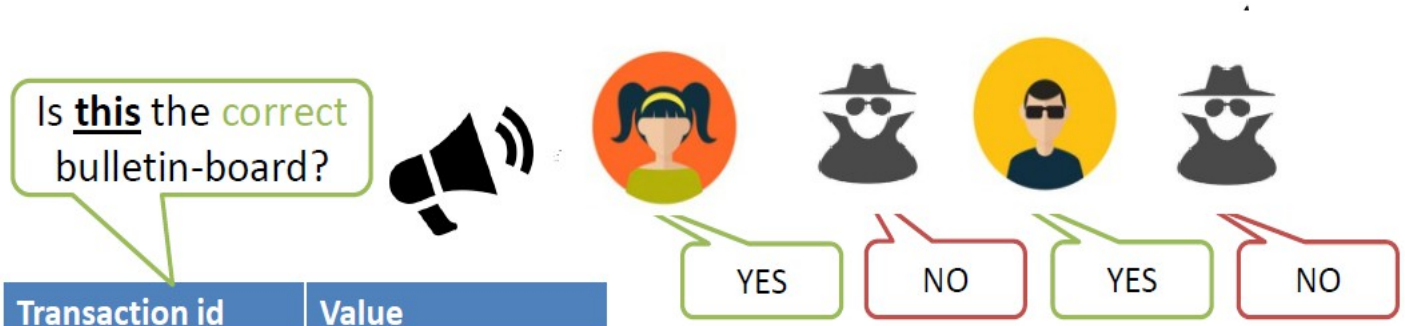
IL CONSENSO IN UN AMBIENTE DISTRIBUITO



- diverse sfide:
  - nodi maliziosi o gusti
  - presenza di jitter, delay, di rete
- un risultato classico: se la "maggioranza è onesta", il sistema funziona correttamente
  - ma quale nozione di maggioranza?

IL CONSENSO IN UN AMBIENTE DISTRIBUITO

- assumendo una maggioranza onesta
- implementazione del consenso mediante votazione
  - ogni transazione inviata in broadcast sulla rete e si raccolgono i voti



Transaction id	Value
ddbs21239864k...	0.084 BTC
edd98763hn3nr...	1.2 BTC
mkk8765g4g2j3...	0.036 BTC

- come implementare la votazione?
- un problema ben noto nei sistemi distribuiti

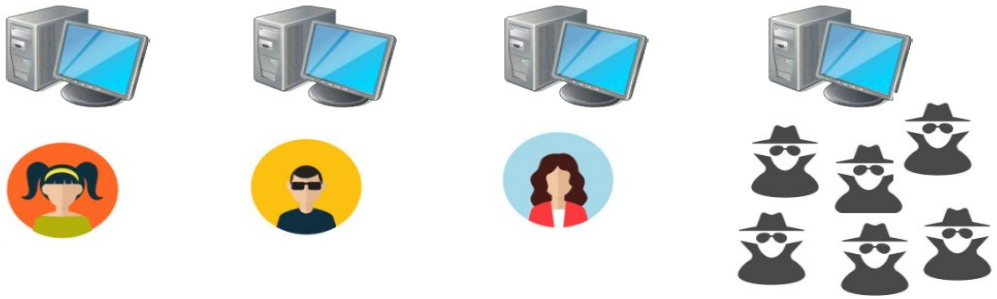
IL TEMIBILE SYBIL ATTACK!!

- Sono la sibilla di Delfi !
- Mi piace molto votare!

CONSENSO E SYBIL ATTACK

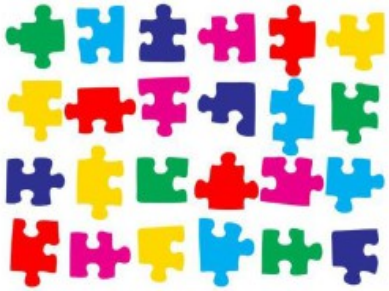
- come definire la maggioranza in un contesto in cui chiunque può unirsi alla rete ed assumere "identità multiple"
  - tipico nelle blockchain a cui ciascun nodo può partecipare, senza restrizioni
  - facile assumere la maggioranza se si controllano più nodi della rete

- maggioranza definita non come maggioranza dei nodi, ma come potere computazionale controllato
  - creare identità multiple non è utile, se poi si ha a disposizione poco potere computazionale

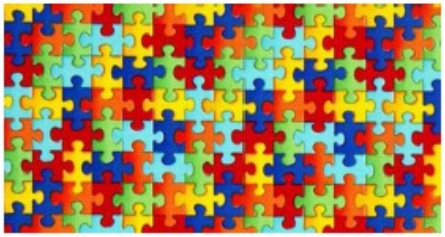


CONSENSO IN BITCOIN

- nessuna votazione esplicita, ma una lotteria
- il miner che risolve la proof of work è quello che decide quale blocco aggiungere alla blockchain
  - richiede la soluzione di un hash puzzle, una problema complesso e che può essere risolto solo in modo combinatorio



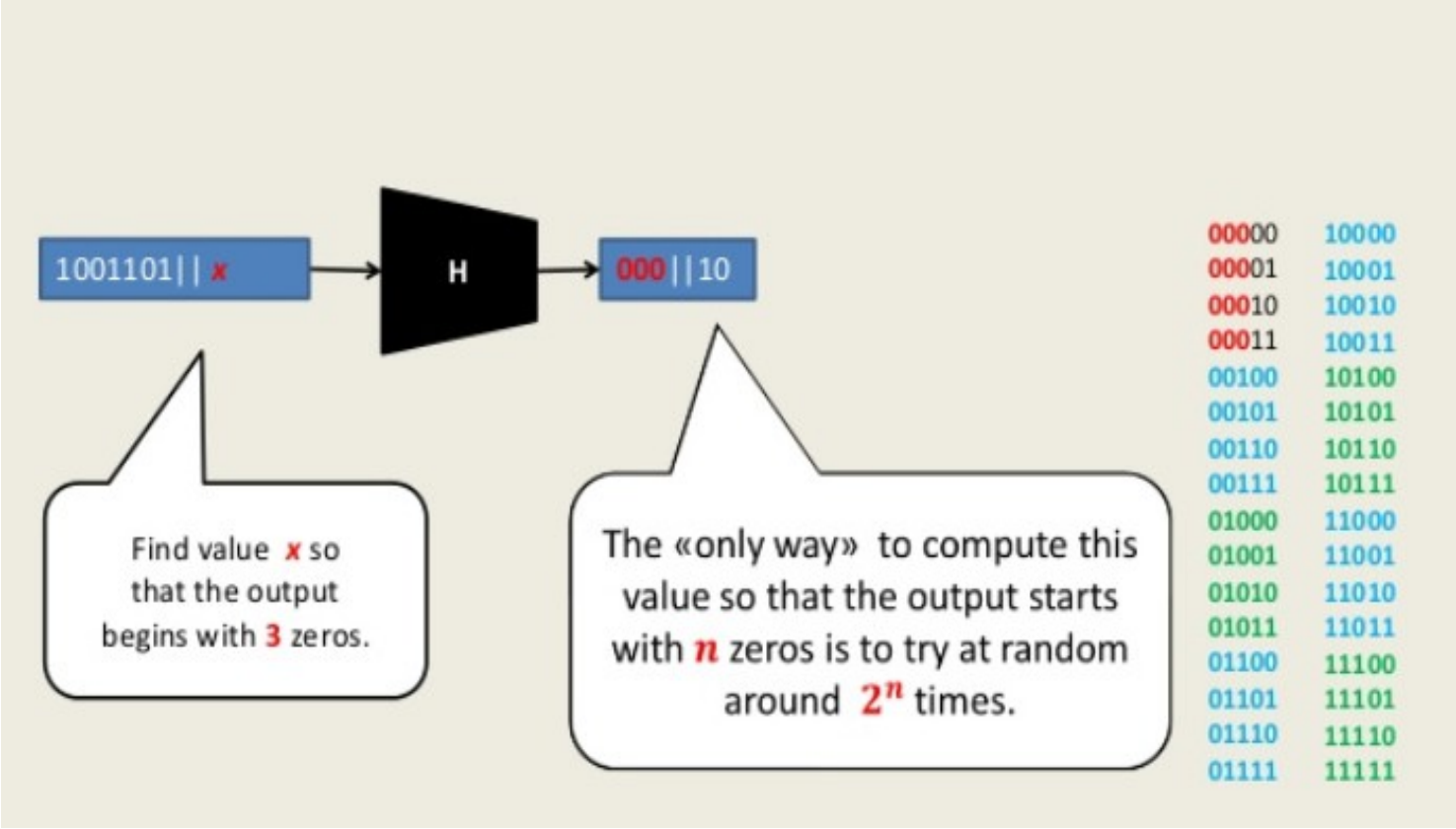
Hard to find solution



Easy to verify

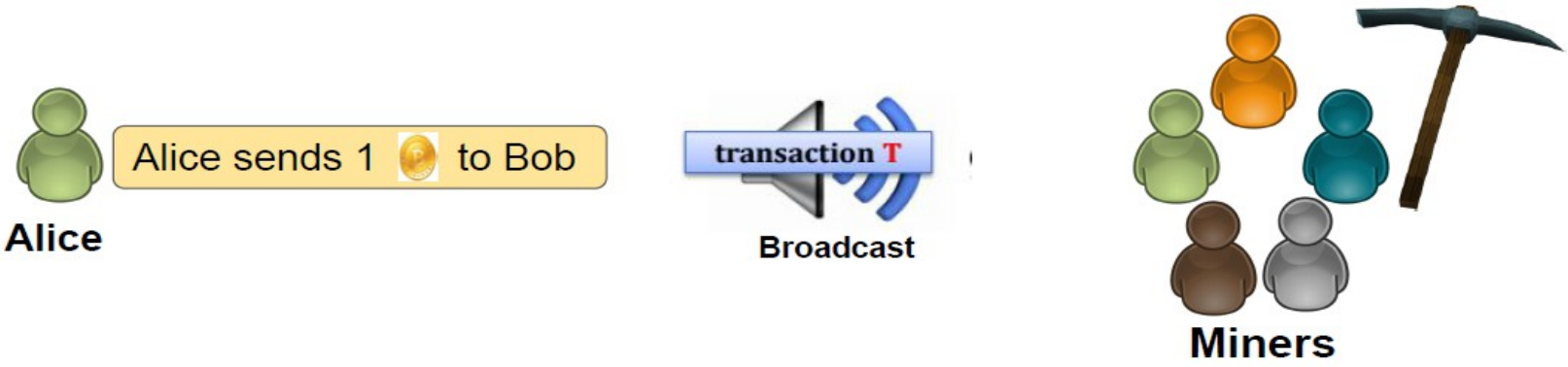
- se la maggioranza del potere computazionale è dei nodi onesti
  - garantito che la blockchain conterrà blocchi validi
  - delay necessario per garantire che i nodi onesti "impongano le loro scelte" in presenza di attacchi da parte dei nodi disonesti

IL PUZZLE CRITTOGRAFICO

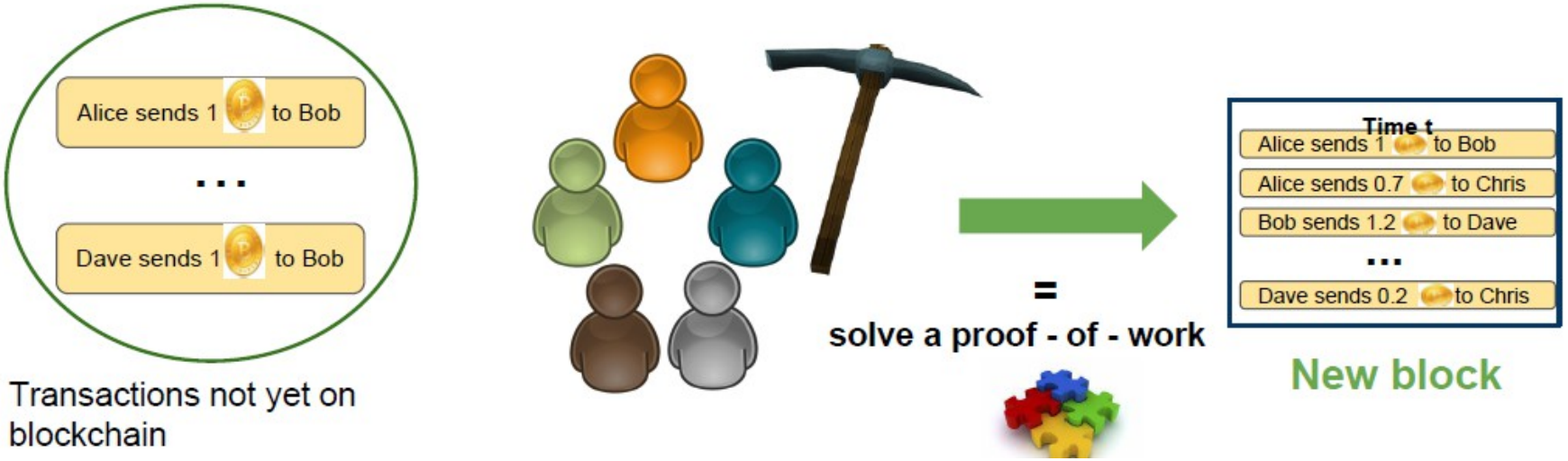


trovare un nonce (x) tale che l'hash di una stringa (che rappresenta un insieme di transazioni) concatenata con il
nonce inizi con un insieme predefinito di zeri

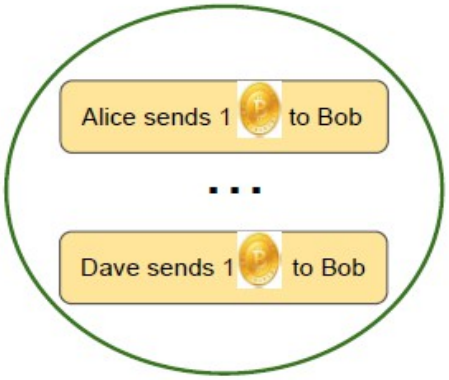
IL PROCESSO DI MINING DI BITCOIN



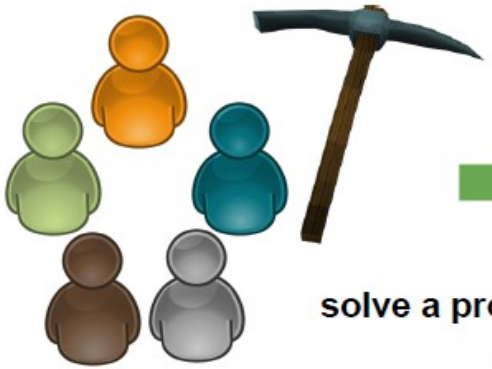
I miners competono in una gara per decidere chi inserirà il prossimo blocco



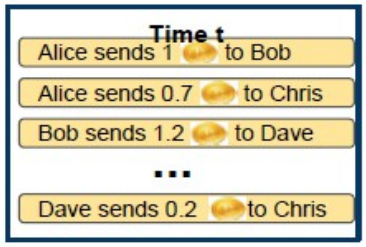
IL PROCESSO DI MINING DI BITCOIN



Transactions not yet on blockchain



= solve a proof - of - work



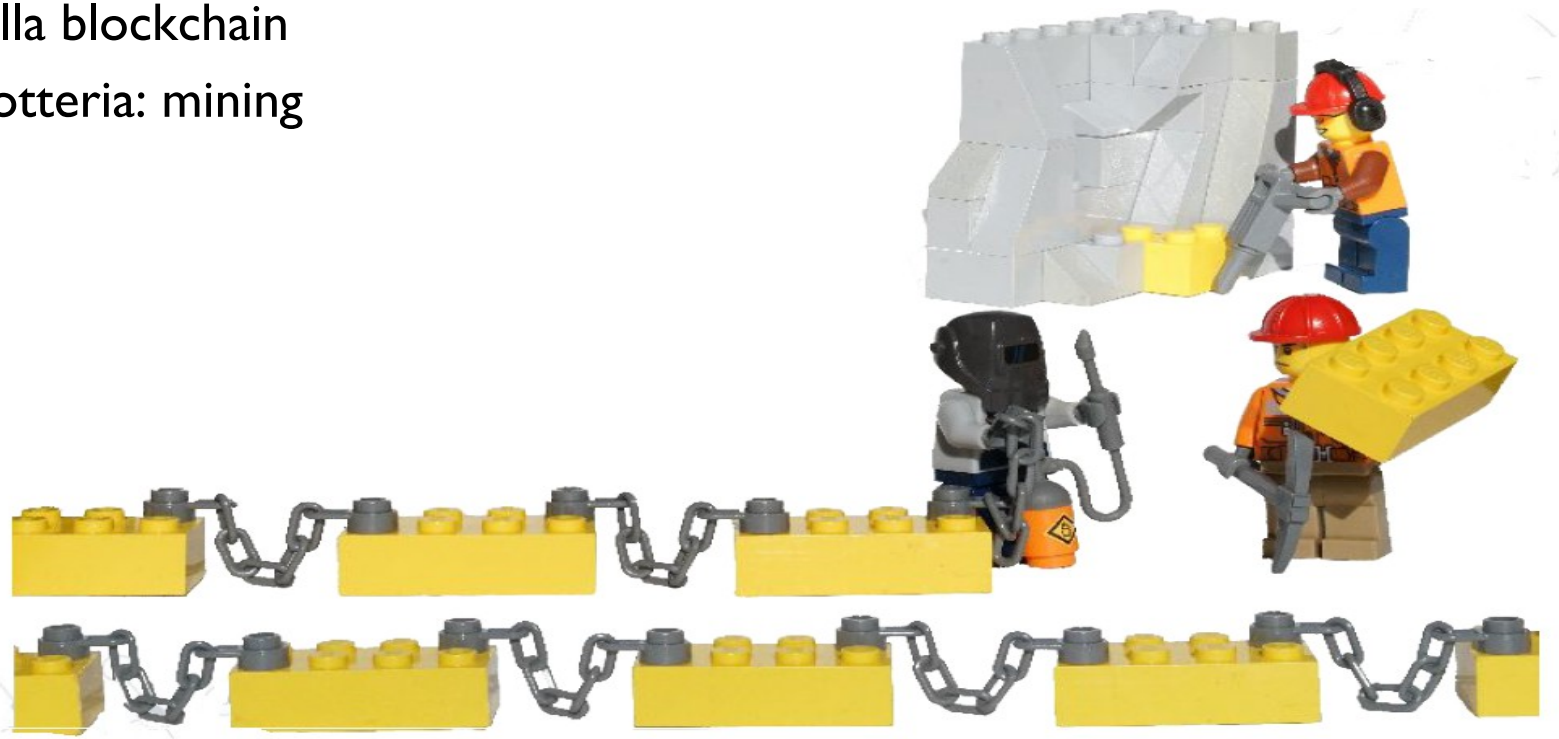
New block

I found a new block!

And to other nodes

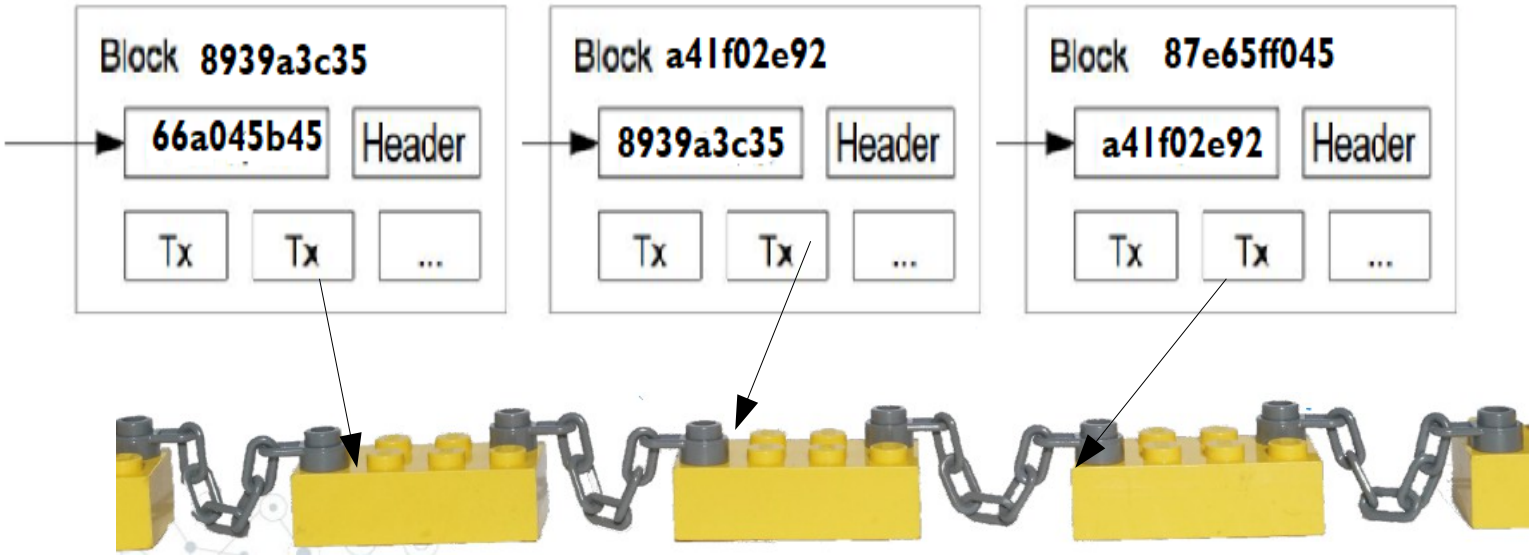
IL CONSENSO IN BITCOIN

- chi aggiunge blocchi alla catena?
  - senza alcun controllo le diverse copie diventano incoerenti
- in Bitcoin:
  - tutti partecipano ad "una lotteria"
  - solo chi vince (e vincere è complesso), può appendere il prossimo blocco alla blockchain
  - lotteria: mining



LA BLOCKCHAIN

- i blocchi della blockchain sono indentificati dall'hash del loro contenuto
  - contenuto: insiemi di transazioni + un header
- blockchain
  - catena in cui ogni blocco memorizza l'hash del blocco precedente
  - puntatori hash formano la catena



TANTI MODELLI PER LE BLOCKCHAIN

- la blockchain di cui abbiamo parlato fino adesso è quella di riferimento, di Bitcoin
- ma sono possibili modelli diversi
  - permissioned/permissionless
  - private/public
- diversimeccanismo di accesso e di consenso

TANTI MODELLI PER LE BLOCKCHAIN

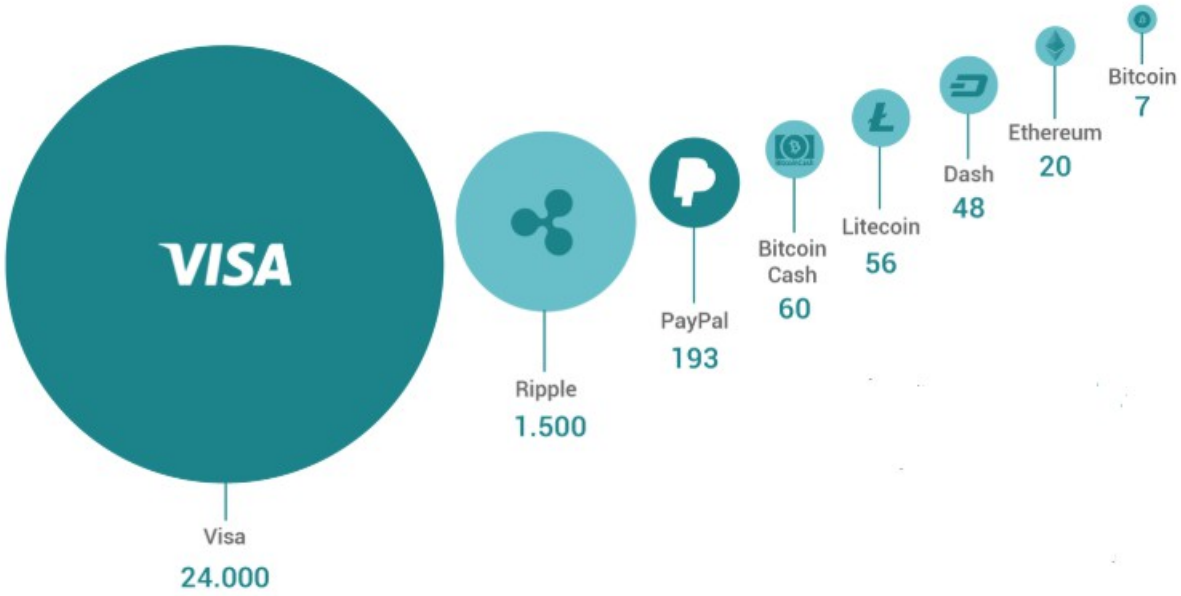
	Permissionless (Qualsiasi utente può partecipare alla rete e validare le transazioni)	**Permissioned** (Solo alcuni utenti hanno il diritto di validare le transazioni)
Pubblica (Tutti gli utenti possono leggere i dati)	• Ogni utente può leggere i dati delle transazioni. • Ogni utente può validare le transazioni. Esempio: Bitcoin ed Ethereum	• Ogni utente può leggere i dati delle transazioni. • Solo utenti autorizzati possono validare le transazioni. Esempio: una blockchain Permissioned in cui si decide di rendere pubblici i dati delle transazioni
Privata (Accesso ai dati limitato ad utenti autorizzati)	• Solo utenti autorizzati possono leggere i dati delle transazioni. • Ogni utente può validare le transazioni. Esempio: Ethereum permette di creare istanze private	• Solo utenti autorizzati possono leggere i dati delle transazioni. • Solo utenti con diritti speciali possono validare le transazioni. Esempio: Hyperledger Fabric

E MOLTE SFIDE DA AFFRONTARE

- scalabilità
  - gestire *grandi quantità* di "transazioni" in *breve tempo*
- interoperabilità
  - scambiare dati tra piattaforme diverse, e con il mondo off-chain
    - far "comunicare" blockchain di tipo diverso
    - definizione di un protocollo comune?
- sostenibilità
  - elevato costo del mining in Bitcoin
  - definizione di diversi algoritmi di consenso
- privacy
  - cosa mettere sulla blockchain? quali dati devono rimanere privati?

LA SCALABILITA'

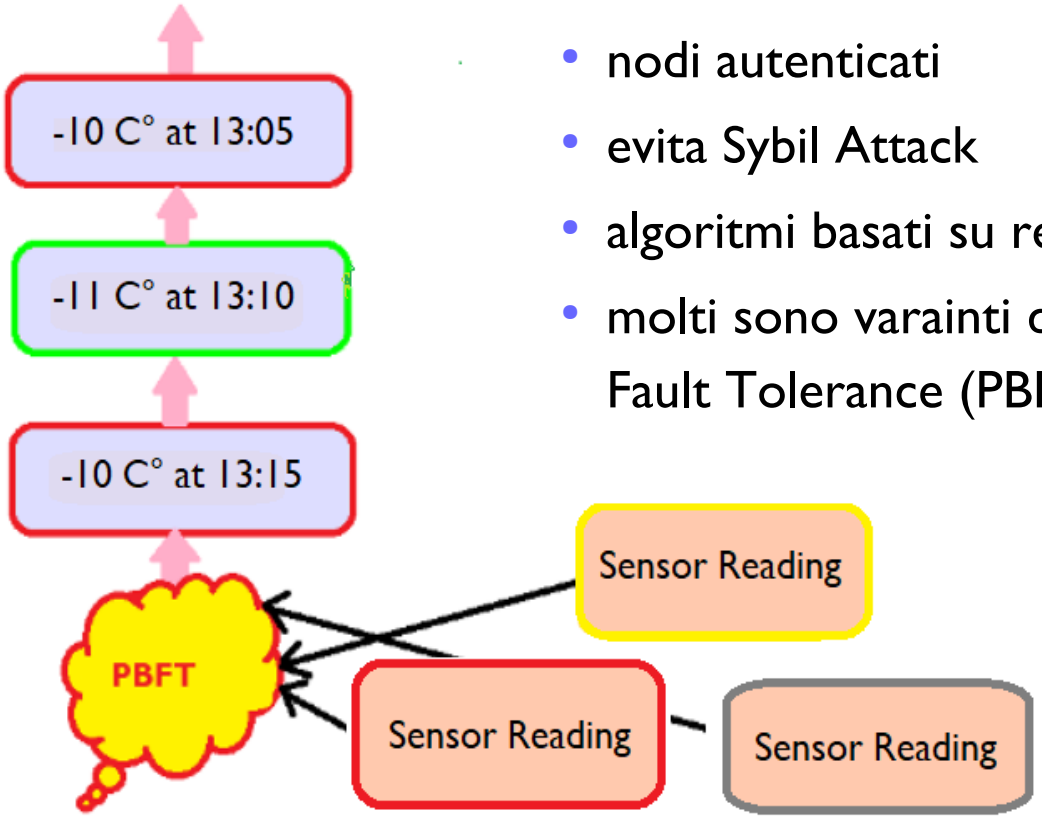
- capacità di gestire grandi quantità di transazioni in maniera reattiva, in breve tempo
- quante transazioni? dipende dal contesto applicativo....
- l'esempio delle criptomonete:



LA SOSTENIBILITA'

- consenso basato su Proof of Work: richiede grosso investimento per il pagamento di elettricità
- quali contro-misure per la riduzione dell'impatto energetico?
  - server farm in locazioni in cui l'energia è meno costosa, abbondante o green
  - riciclo dell'energia generata dai server per il riscaldamento di edifici
  - utilizzo di energia elettrica in eccesso, quindi non stoccabile
- soluzioni per scalabilità e sostenibilità: definizione di nuovi algoritmi di consenso
  - Proof of Stake
  - Byzantine Agreements
  - ….una "giungla" di proposte

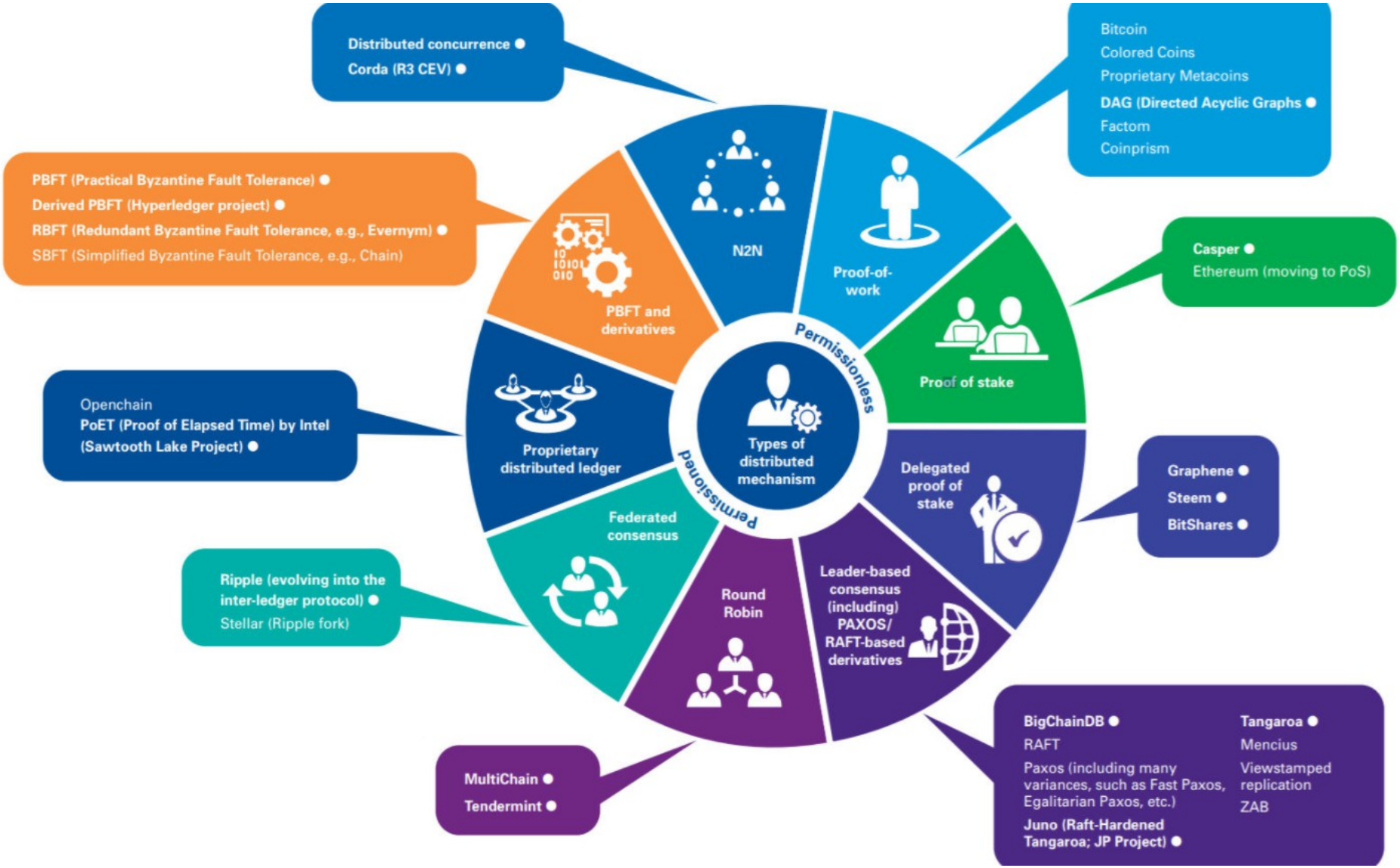
PERMISSIONED BLOCKCHAIN



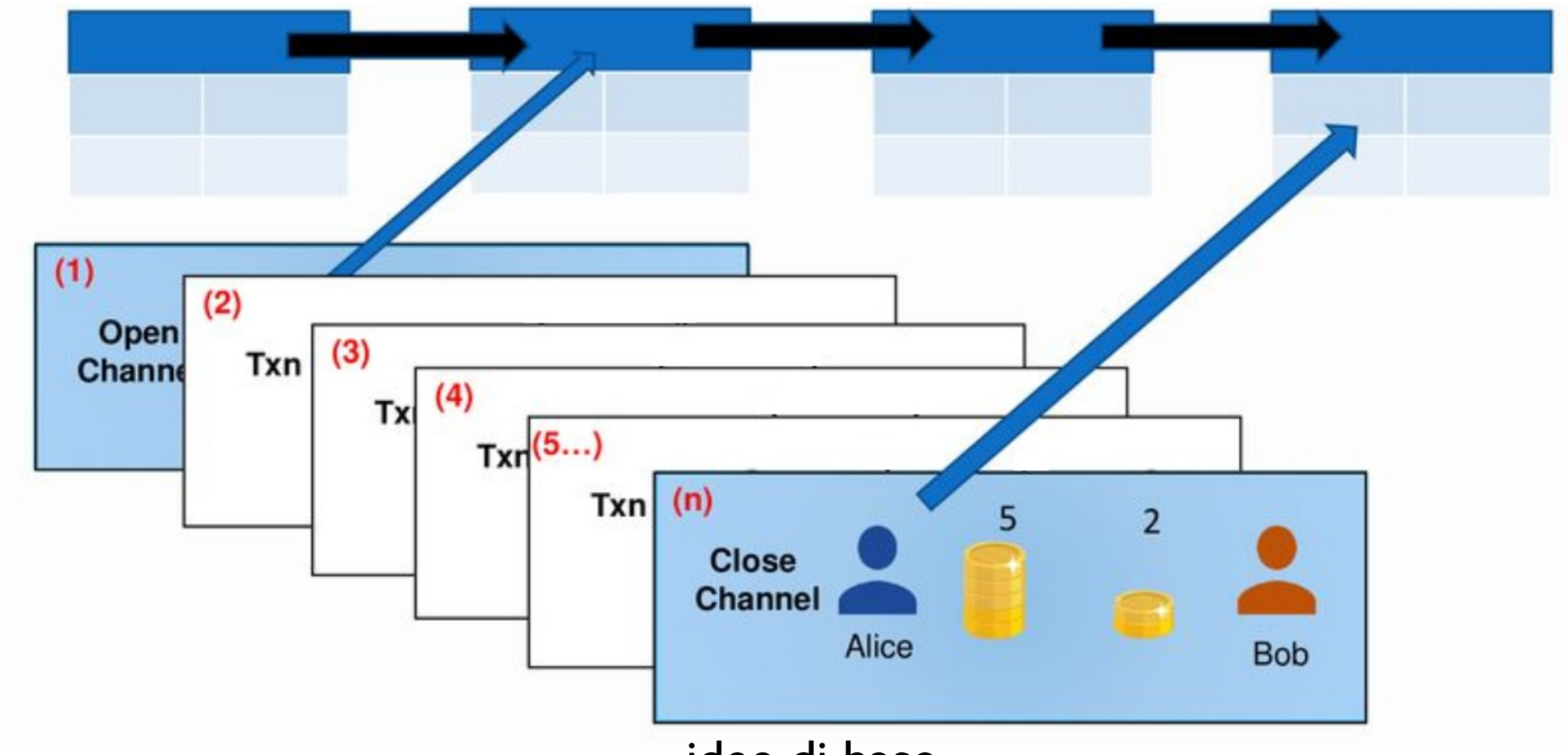
nelle blockchain permissioned

- nodi autenticati
- evita Sybil Attack
- algoritmi basati su reali votazioni
- molti sono varainti di Practical Blockchain Fault Tolerance (PBFT)

CONSENSO: UN CAMPO ANCORA APERTO...



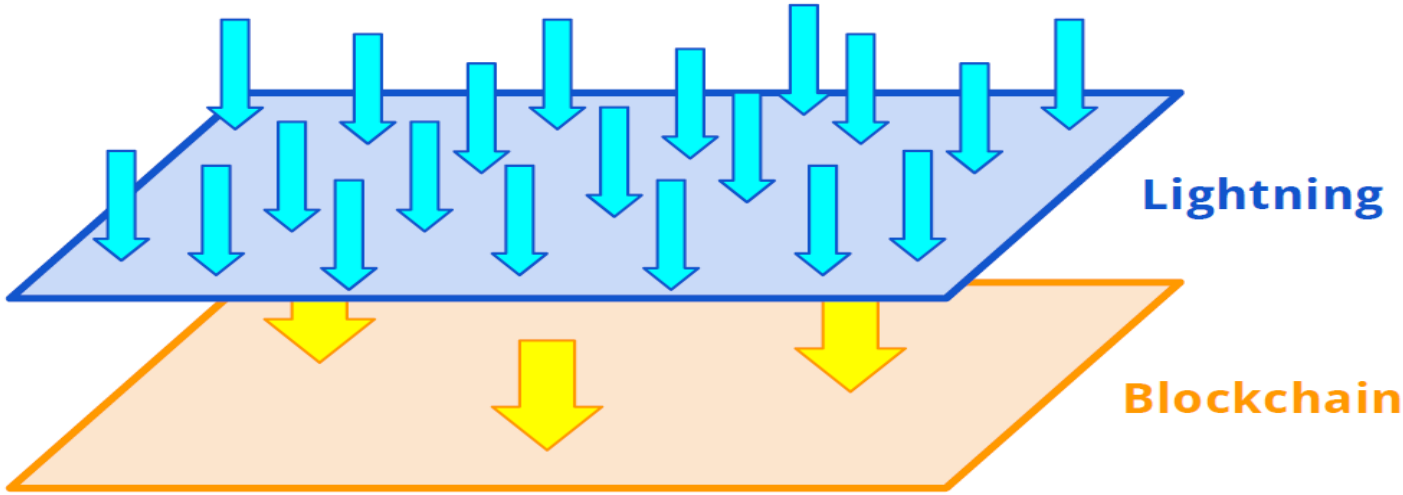
PROBLEMI APERTI: OFF CHAIN CHANNELS



idee di base

- non propagare tutte le transazioni sulla blockchain, ma usare canali off-chain
- la blockchain come "arbitro"
  - Solo transazioni di apertura e chiusura canale on-chain

LA LIGHTNING NETWORK DI BITCOIN



- Lightning network: un overlay P2P di Layer-2, definito sopra la blockchain
- Diversi problemi aperti
  - algoritmi di routing sulla rete di livello-2
  - multi-path payment: split di un pagamento su più cammini
  - studio della topologia della Lightning Network come rete complessa

PROBLEMI APERTI: L'ECOSISTEMA CRYPTO

- crypto-exchange
  - cambio tra valute diverse
- caratterizzati da diversi livelli di affibilità
- spunto di ricerca
  - sviluppo di tecniche per la valutazione della affidabilità
  - scraping web
  - raccolta dati tramite API degli exchange

PROBLEMI APERTI: BLOCKCHAIN SOCIAL NETWORKS

- Steemit, una social network basata sulla Steem Blockchain
- un nuovo modello di socialità
  - membri ottengono premi dal sistema per le attività svolte
  - upvote e downvote a post originali
  - diverse forme di valuta interne al sistema
- problemi aperti:
  - analizzare relazione tra socialità e ricompense
  - il valore è realmente distribuito o è a disposizione di pochi utenti?
  - Influenza dei bot sulla piattaforma

PROBLEMI APERTI: PRIVACY

- utilizzo di tecniche crittografiche avanzate
  - Zero-knowledge
  - Multi Signatures
  - Diffie Helmann
  - Blind Signatures
  - Accumulatori

- costo computazionle
- quale implementazione?
- collaborazioni
  - dipartimento professoressa Anna Bernasconi
  - IIT CNR: dottor Paolo Mori

RIFERIMENTI

- corso *P2P & Blockchain,* Laurea Magistrale in informatica, Curriculum ICT
- possibilità di tirocini triennali e tesi di Laurea Magistrale
- un nutrito gruppo di ricercatori:
  - *Laura Ricci*
  - *Fabrizio Baiardi (aspetti di sicurezza)*
  - Paolo Mori (CNR, IIT, Pisa)
  - Barbara Guidi
  - Damiano di Francesco Maesa (University of Cambridge)
  - Andrea De Salve (ISASI, CNR, Lecce)
  - Andrea Michienzi (Dottorando)
  - Andrea Lisi (Dottorando)
  - Mohsin Ur-Rahman (Dottorando)
  - Adrian Spataru (Dottorando)
  - Matteo Loporchio (Dottorando)

LA MIA ESPERIENZA AL MISE

- Gennaio 2019- Settembre 2020
- MISE Ministero dello Sviluppo Economico
- un gruppo di esperti che ha riunito
  - accademici
  - industria
  - parti sociali
- con diversi background
  - tecnologico
  - giuridico
  - economico
- strategia posta in consultazione popolare a Giugno 2020
- versione definitiva pubblicata a breve

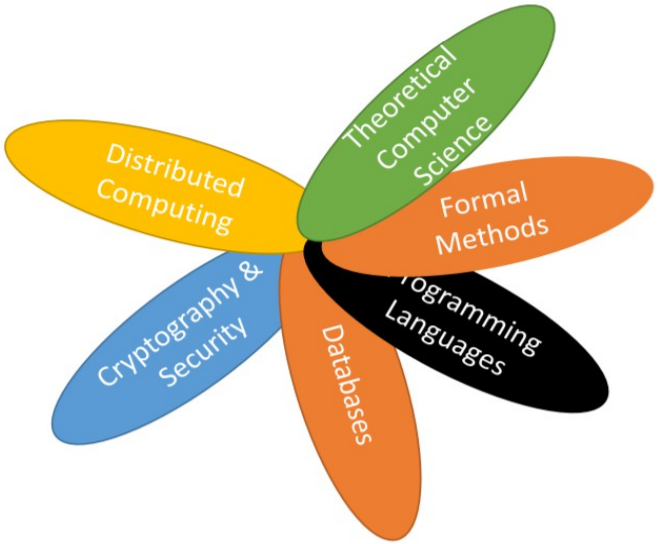
RIFERIMENTI

spunti per tirocini/tesi di laurea magistrale

- applicazione di tecniche crittografiche a blockchain
- bot discovery: analisi delle transazioni
- analisi di blockchain di ultima generazione
  - EOS
  - Algorand proposto da *"Silvio Micali, the geinus of computer science who wants to make blockchain more efficient" Forbes, October 2018"*
    - Algorand Europe Accellerator for start-ups
  - Stellar
  - Ethereum 2.0
- scalabilità
  - lightning network: progettazione di algoritmi di rotuing ad hoc
  - sharding

CONCLUSIONI: HYPE O REALTA'?

- "The blockchain will do to the financial system what the internet did to media" *Joi Ito, Neha Narula and Robleh Ali - Harvard Business Review*
- "I think [blockchain] is a fascinating area to keep an eye out for, but I think it's being over-hyped right now… from the aspect of its short-term impact because there are still technical things that you need to solve and scale and there are still counter-aspects – business model wise – that aren't necessarily fully clear." *Peter Sondergaard, SVP Technology, Gartner*



Molti problemi da risolvere:

e le sfide tecniche sono complesse!

diverse aree della computer science sono coinvolte

BLOCKCHAIN @INFORMATICA

- non aggiornato, causa COVID
- + 2 nuovi dottorandi: Andrea Lisi, Matteo Loporchio (collaborazione con la professoressa Bernasconi)