DISTRIBUTED LEDGERS: OLTRE LE CRYPTOCURRENCIES

Laura Ricci
Dipartimento di Informatica,
Università degli Studi di Pisa

Roma, 19 giugno 2019
Sala Spadolini
Ministero per i Beni e le Attività Culturali
Via del Collegio Romano 27

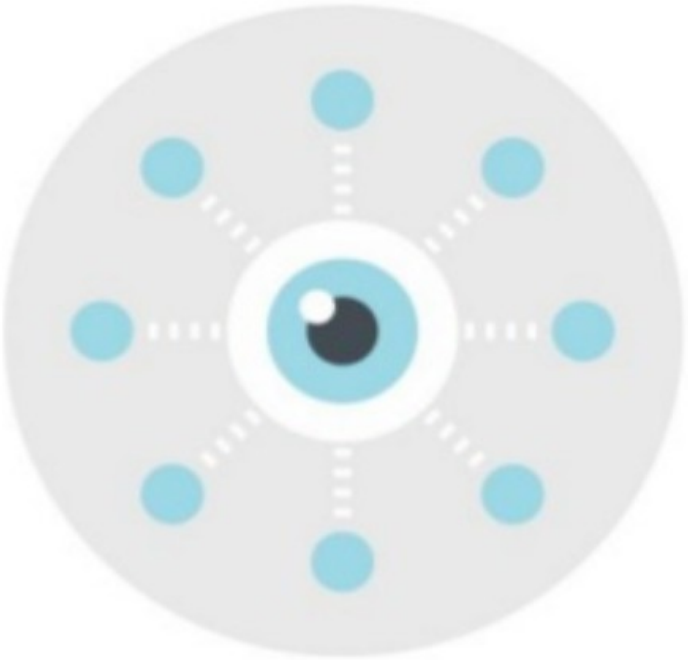
INTRODUZIONE

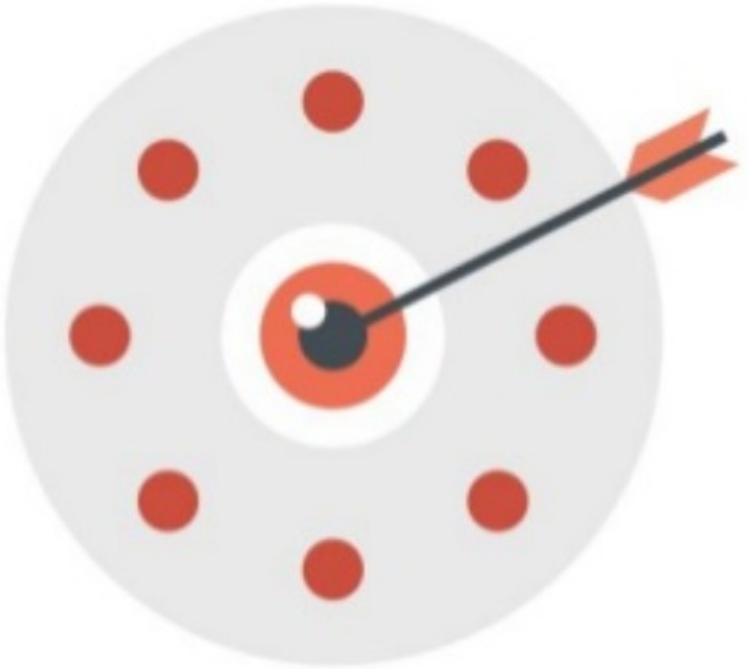
- ma le blockchain sono veramente utili?
- urgente fornire maggior consapevolezza
- più formazione, più ricerca
- stiamo lavorando insieme, a Pisa, computer scientists, giuristi su diversi
- aspetti
  - progetti europei H2020 e progetti nazionali (PRIN,...)
  - contatti con le industrie locali
  - corsi congiunti in lauree magistrali

BLOCKCHAIN @INFORMATICA, PISA

ELIMINARE LA CENTRALIZZAZIONE

un sistema centralizzato

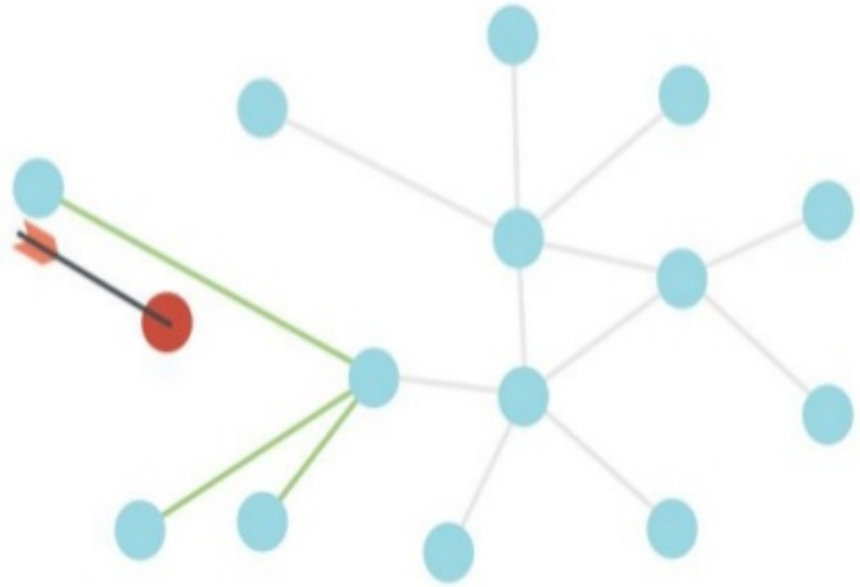




Informazione e controllo in una unica entità centralizzata

Se l'entità centralizzata fallisce/ è sottoposta a censura/ è corrotta, tutto il sistema smette di funzionare

SISTEMI DISTRIBUITI O PEER TO PEER



non esiste un'entità centralizzata,
ma una rete di nodi

reti peer to peer: rapporto tra nodi pari a pari

se un nodo fallisce/è sottoposto a censura, è corrotto, la rete continua a funzionare, si "auto-ripara"

REGISTRI DISTRIBUITI: DEFINIZIONE

- un database distribuito e replicato sui nodi di un sistem peer to peer
  - ogni peer possiede una copia coerente dell'intero database
  - non una sola entità centrale che gestisce i dati
- operazioni possibili sul database
  - accodare progressivamente registrazioni
  - leggere il contenuto di una qualsiasi registrazione
  - immutabilità (tamper freeness)
    - nessuno può modificare una registazione scritta in precedenza (neppure l'amministratore di sistema)
    - proprietà garantita da un protocollo crittografico

REPLICAZIONE E CONSENSO

- distribuzione dei dati: ogni peer (nodo) del sistema ha la stessa copia del database
- condivisione di un'unica copia dei dati, uguale su tutti i peer
- si evitano:
  - svantaggi della centralizzazione
  - gestione di database contenenti dati diversi/sviluppati con tecnologie diverse
  - aggiornamento di copie multiple
    - un'unica copia per tutti
    - una visione unica dei dati sui vari nodi

MECCANISMO DI CONSENSO

- i dati che vengono aggiunti alla blockchain devono essere "approvati" dalla maggioranza dei peer
  - definizione di algoritmi per il consenso, tutti devono essere d'accordo sul valore da aggiungere al registro
    - distributed lottery per Bitcoin
    - generali bizantini per blockchain permissioned.
- un dato approvato dalla maggioranza dei peer è aggiunto nella blockchain di tutti i peer
  - è necessario che la maggioranza sia onesta
  - conviene davvero essere disonesti: teoria dei giochi?

TRANSAZIONI

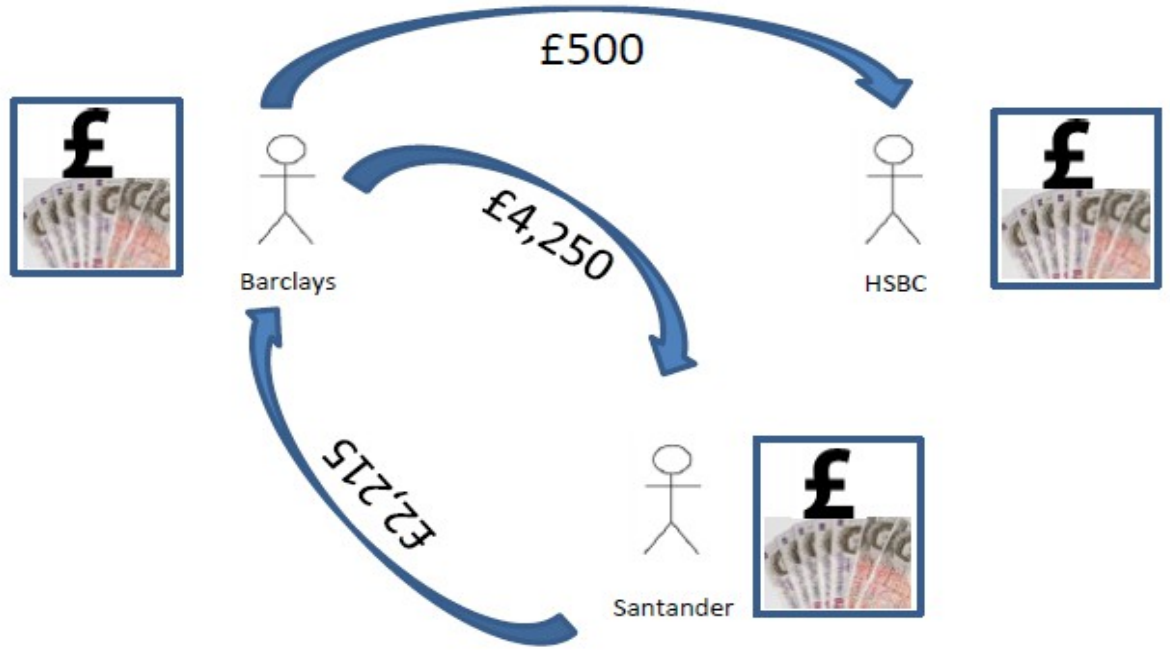
- supponiamo che il database distribuito registri un insieme di operazioni o transazioni
- transazione
  - Bitcoin, trasferimento di una somma di denaro tra due entità
  - ma non solo
    - un contratto tra due parti
    - la fruizione di un contenuto (canzone, video,..)
    - concessione del diritto ad accedere ad alcuni dati sensibili
    - una offerta al rialzo in un'asta online

LEDGER: IL LIBRO MASTRO DELLE TRANSAZIONI

JOURNAL -ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
1	01/01/2016 08:35	BARCLAYS	HSBC	GBP	500.00

LEDGER: IL LIBRO MASTRO DELLE TRANSAZIONI

BARCLAYS JOURNAL					
JOURNAL-ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
1	01/01/2016 08:35	BARCLAYS	HSBC	GBP	500.00
2	01/01/2016 09:45	BARCLAYS	SANTANDER	GBP	4,250.00
3	01/01/2016 11:35	SANTANDER	BARCLAYS	GBP	2,215.00



Dove e come memorizzare questo database?

TANTI LEDGER, UNO PER OGNI DOMINIO

BARCLAYS JOURNAL					
JOURNAL-ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
1	01/01/2016 08:35	BARCLAYS	HSBC	GBP	500.00
2	01/01/2016 09:45	BARCLAYS	SANTANDER	GBP	4,250.00
3	01/01/2016 11:35	SANTANDER	BARCLAYS	GBP	2,215.00

HSBC JOURNAL					
JOURNAL-ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
1	01/01/2016 08:35	BARCLAYS	HSBC	GBP	500.00
4	01/01/2016 13:35	HSBC	SANTANDER	GBP	105.00

SANTANDER JOURNAL					
JOURNAL-ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
2	01/01/2016 09:45	BARCLAYS	SANTANDER	GBP	4,250.00
3	01/01/2016 11:35	SANTANDER	BARCLAYS	GBP	2,215.00

TANTI LEDGER, UNO PER OGNI DOMINIO

- consistenza:
  - controllare che ogni transazione sia correttamente registrata su ognuno dei ledger
  - evitare informazioni contraddittorie su ledger diversi
  - assume che ci si fidi delle singole amministrazioni

- problemi:
  - gestione interazione tra i vari sistemi
    - manuale
    - automatica: sincronizzazione di applicazioni diversi
  - problemi di trust
  - difficoltà di auditing

UN UNICO LEDGER CONDIVISO

Fondere tutti i ledger e mantenere un unico ledger condiviso....

BARCLAYS JOURNAL					
JOURNAL-ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
1	01/01/2016 08:35	BARCLAYS	HSBC	GBP	500.00
2	01/01/2016 09:45	BARCLAYS	SANTANDER	GBP	4,250.00
3	01/01/2016 11:35	SANTANDER	BARCLAYS	GBP	2,215.00

HSBC JOURNAL					
JOURNAL-ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
1	01/01/2016 08:35	BARCLAYS	HSBC	GBP	500.00
4	01/01/2016 13:35	HSBC	SANTANDER	GBP	105.00

SANTANDER JOURNAL					
JOURNAL-ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
2	01/01/2016 09:45	BARCLAYS	SANTANDER	GBP	4,250.00
3	01/01/2016 11:35	SANTANDER	BARCLAYS	GBP	2,215.00

JOURNAL-ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
1	01/01/2016 08:35	BARCLAYS	HSBC	GBP	500.00
2	01/01/2016 09:45	BARCLAYS	SANTANDER	GBP	4,250.00
3	01/01/2016 11:35	SANTANDER	BARCLAYS	GBP	2,215.00
4	01/01/2016 13:35	HSBC	SANTANDER	GBP	105.00

LA BLOCKCHAIN

Come organizzare il ledger condiviso?

Put the data into blocks and chain them together

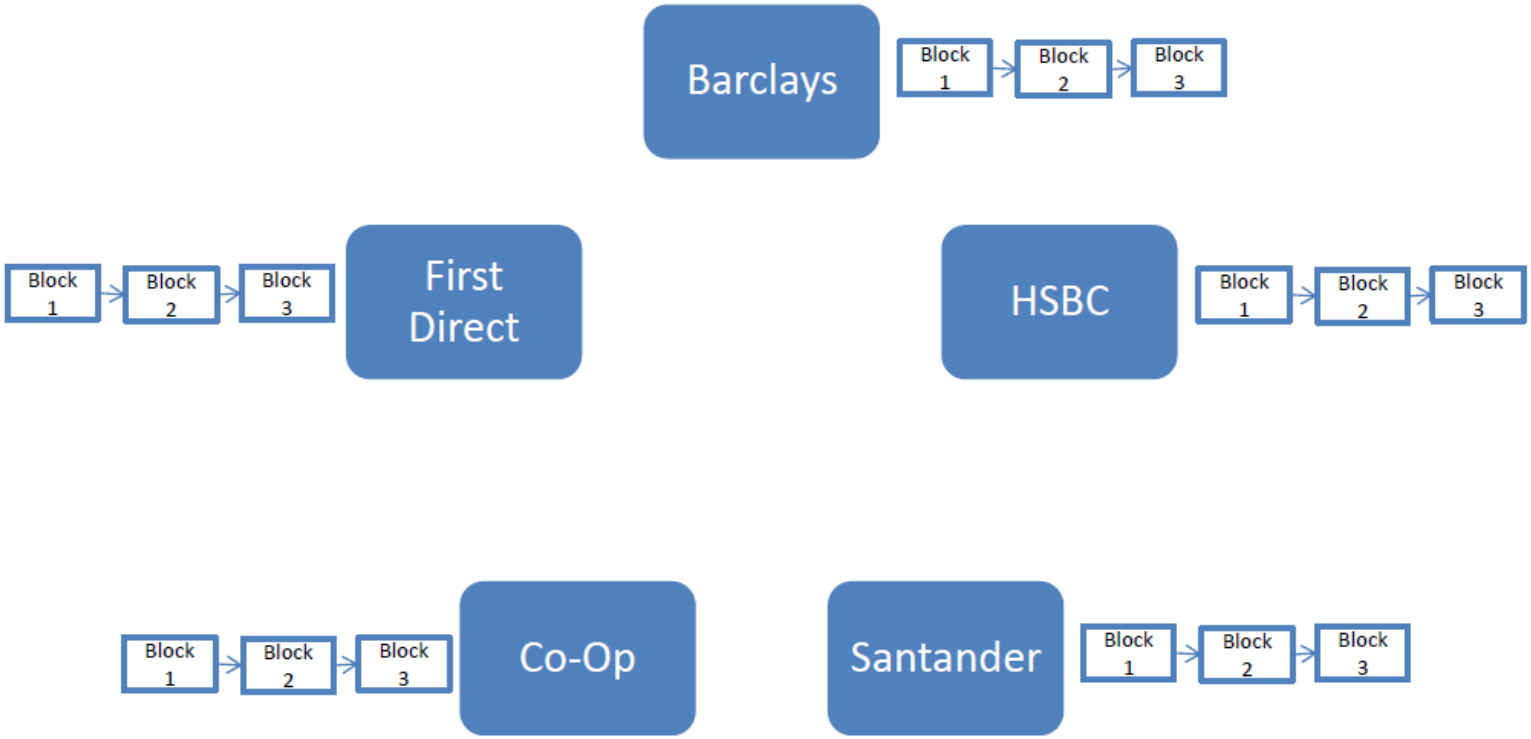
JOURNAL-ID	DATESTAMP	FROM	TO	CURRENCY	AMOUNT
1	01/01/2016 08:35	BARCLAYS	HSBC	GBP	500.00
2	01/01/2016 09:45	BARCLAYS	SANTANDER	GBP	4,250.00
3	01/01/2016 11:35	SANTANDER	BARCLAYS	GBP	2,215.00
4	01/01/2016 13:35	HSBC	SANTANDER	GBP	105.00

BLOCK 1				BLOCK 2				BLOCK 3		
DATA	PREV HASH	CURRENT HASH		DATA	PREV HASH	CURRENT HASH		DATA	PREV HASH	CURRENT HASH
1	1011	1100		1	1100	1101		1	1101	1111

Blockchain

LA BLOCKCHAIN: MEMORIZZAZIONE

- dove memorizzare la blockchain (ledger)?
- ogni peer della rete memorizza una copia del ledger
  - replicazione dei dati



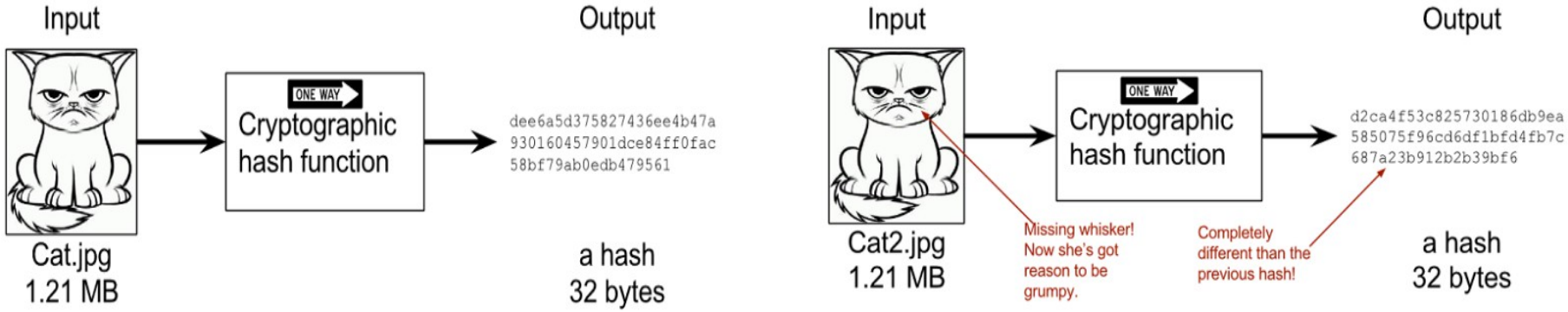
UN PO' DI DETTAGLI "TECNOLOGICI"

occorre garantire due proprietà:

- immutabilità dei dati:
  - come garantire l'immutabilità in modo automatico? due idee di base:
    - hash
    - proof of work
- coerenza: tutti devono avere la stessa copia della blockchain
  - algoritmi di consenso
    - proof of work
    - proof of stake
    - bizantine consensus

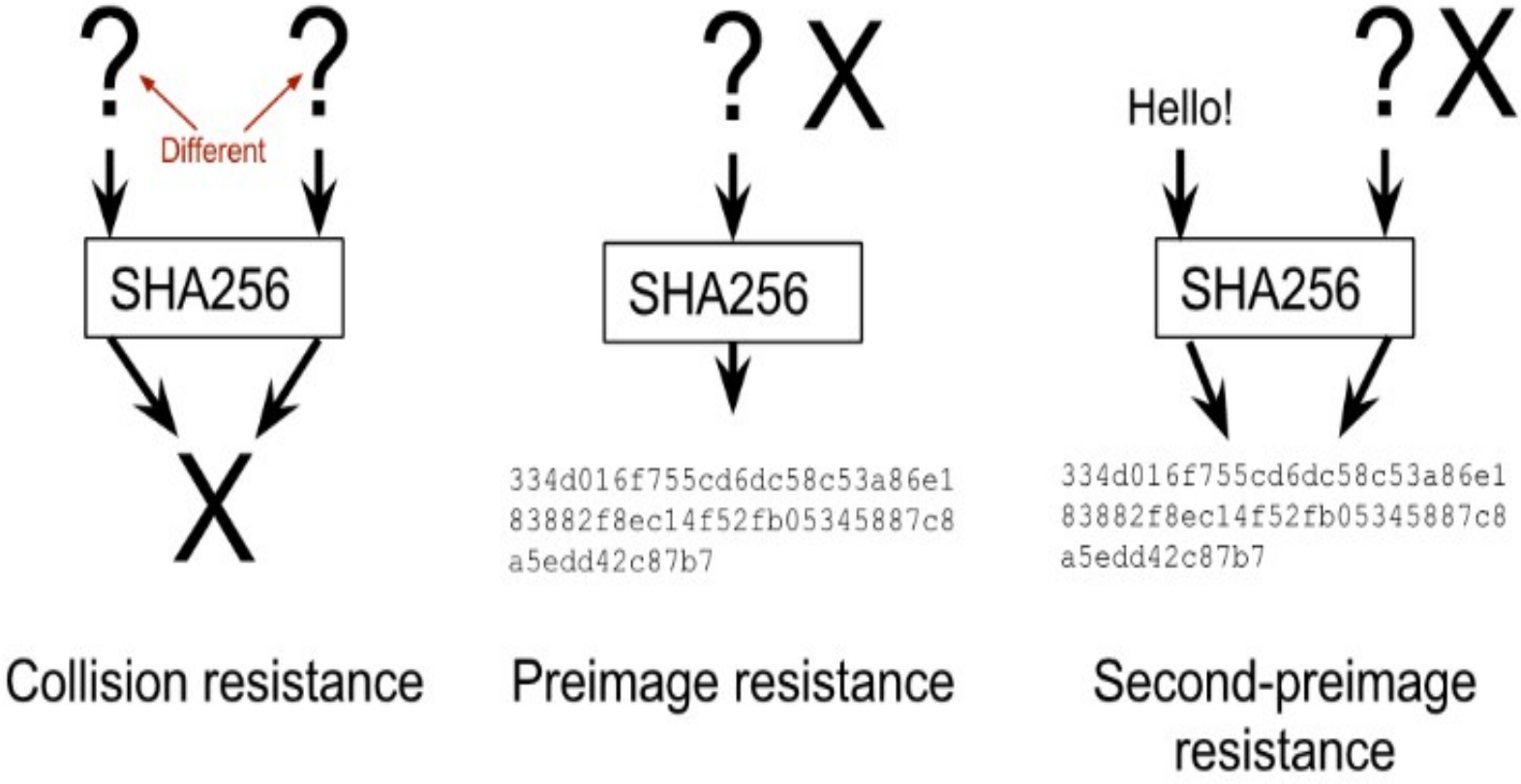
FUNZIONI HASH CRITTOGRAFICHE

- un tipo di funzione matematica che associa a dati di qualsiasi lunghezza un'"impronta digitale" (fingerprint) di lunghezza fissa



- dati in input : qualsiasi lunghezza, qualsiasi tipo
- dati in output:
  - sequenza di caratteri di dimensione fissata
  - se cambio anche leggermente l'input, l'output cambia completamente

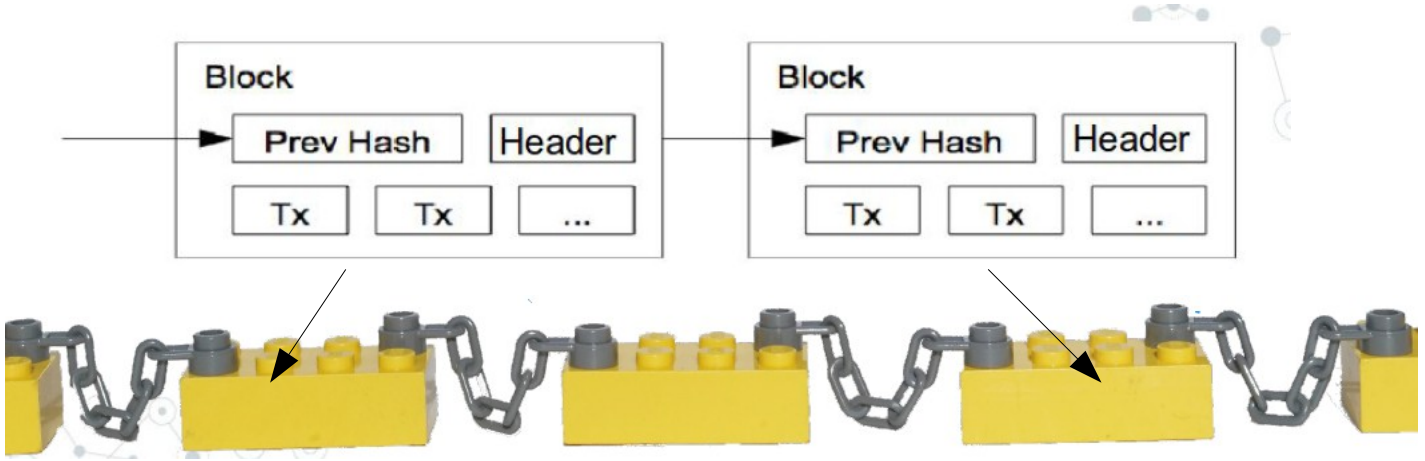
FUNZIONI HASH CRITTOGAFICHE: PROPRIETA'



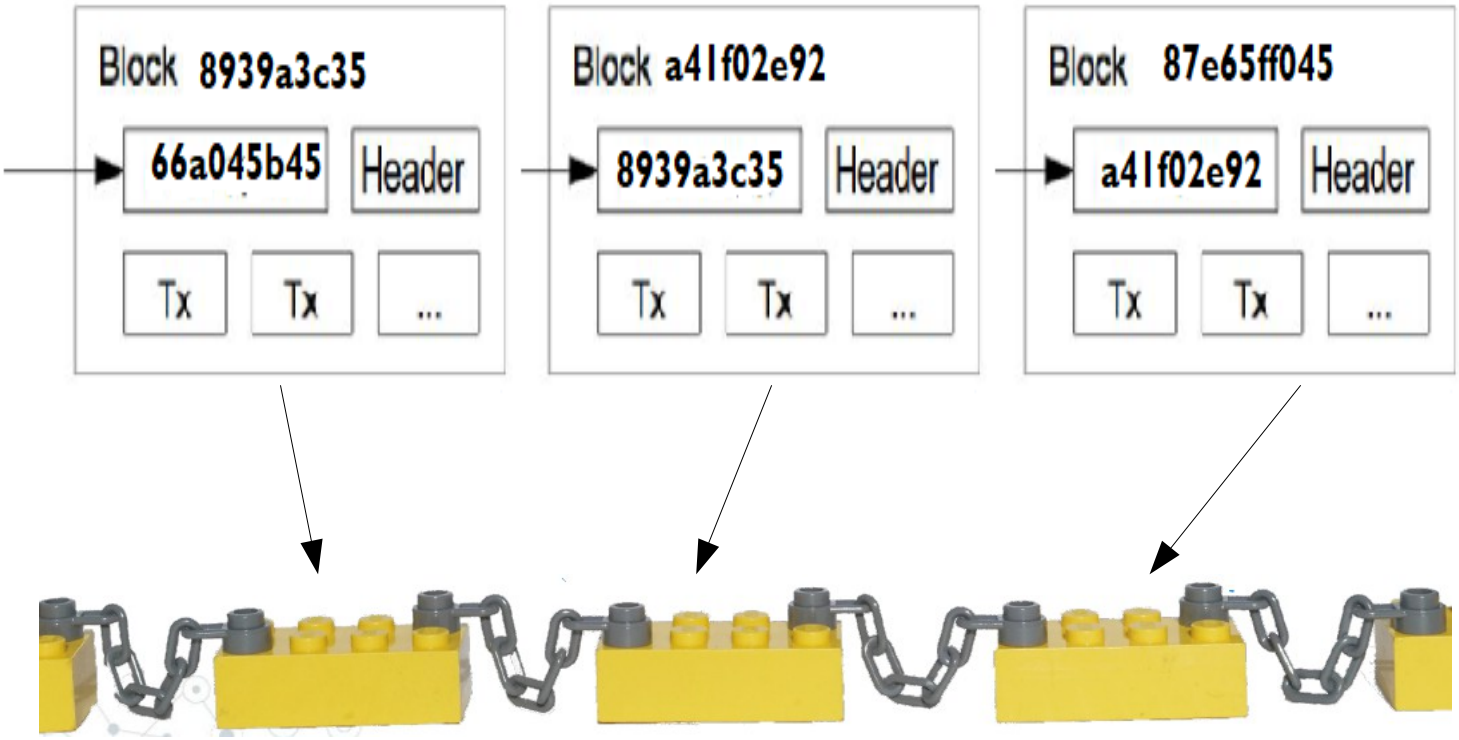
- SHA-256/512 (for Secure Hash Algorithm – 256 bit), uno standard consolidato che garantisce le precedenti proprietà

UN PO' DI DETTAGLI "TECNOLOGICI": BLOCCHI

- blocchi:
  - insiemi di transazioni +header
  - ad ogni blocco viene associato un hash
  - l'hash del blocco è calcolato a partire dal contenuto del blocco (non un semplice numero progressivo)
- blockchian: ogni blocco memorizza l'hash del blocco precedente
  - si forma una catena (chain) di blocchi

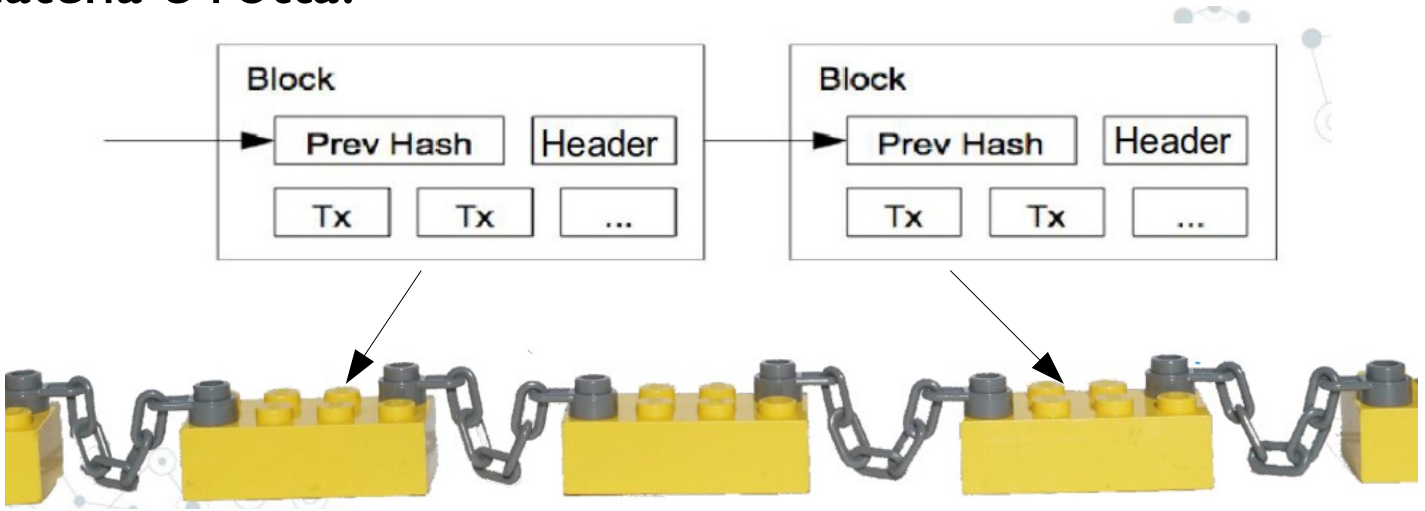


LA BLOCKCHAIN: UN ESEMPIO



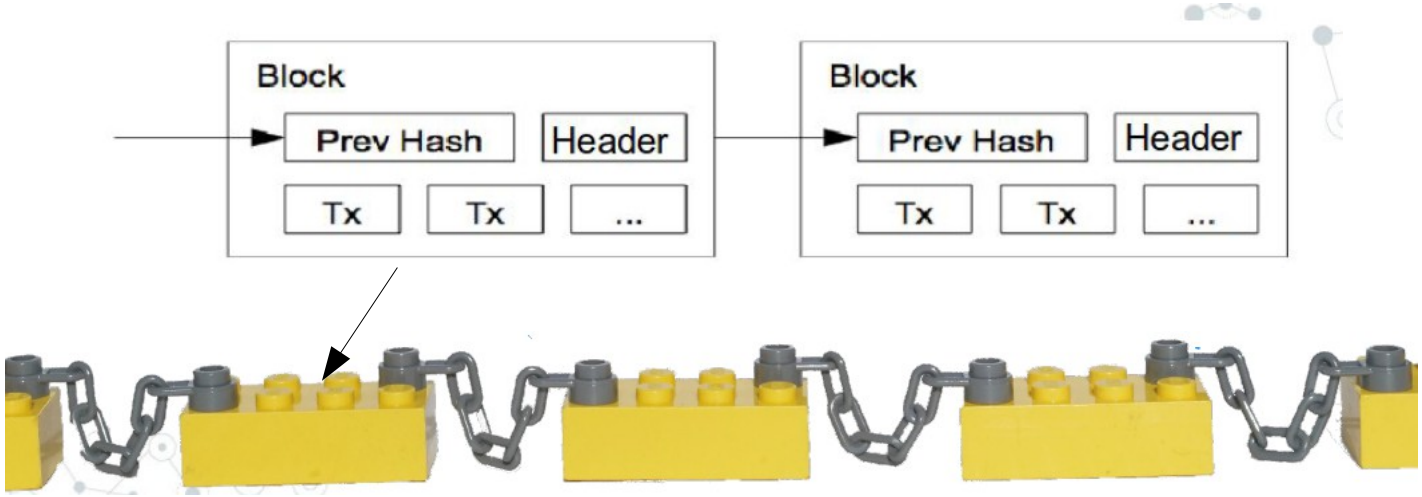
BLOCKCHAIN: IMMUTABILITA'

- non una semplice numerazione progressiva dei blocchi, come quella delle pagine di un libro!
- hash dipende dal contenuto del blocco
  - se cambio il contenuto del blocco B, cambio il suo hash
  - l'hash di B è memorizzato nel blocco successivo
  - devo cambiare il blocco successivo e così via...
  - la catena è rotta!



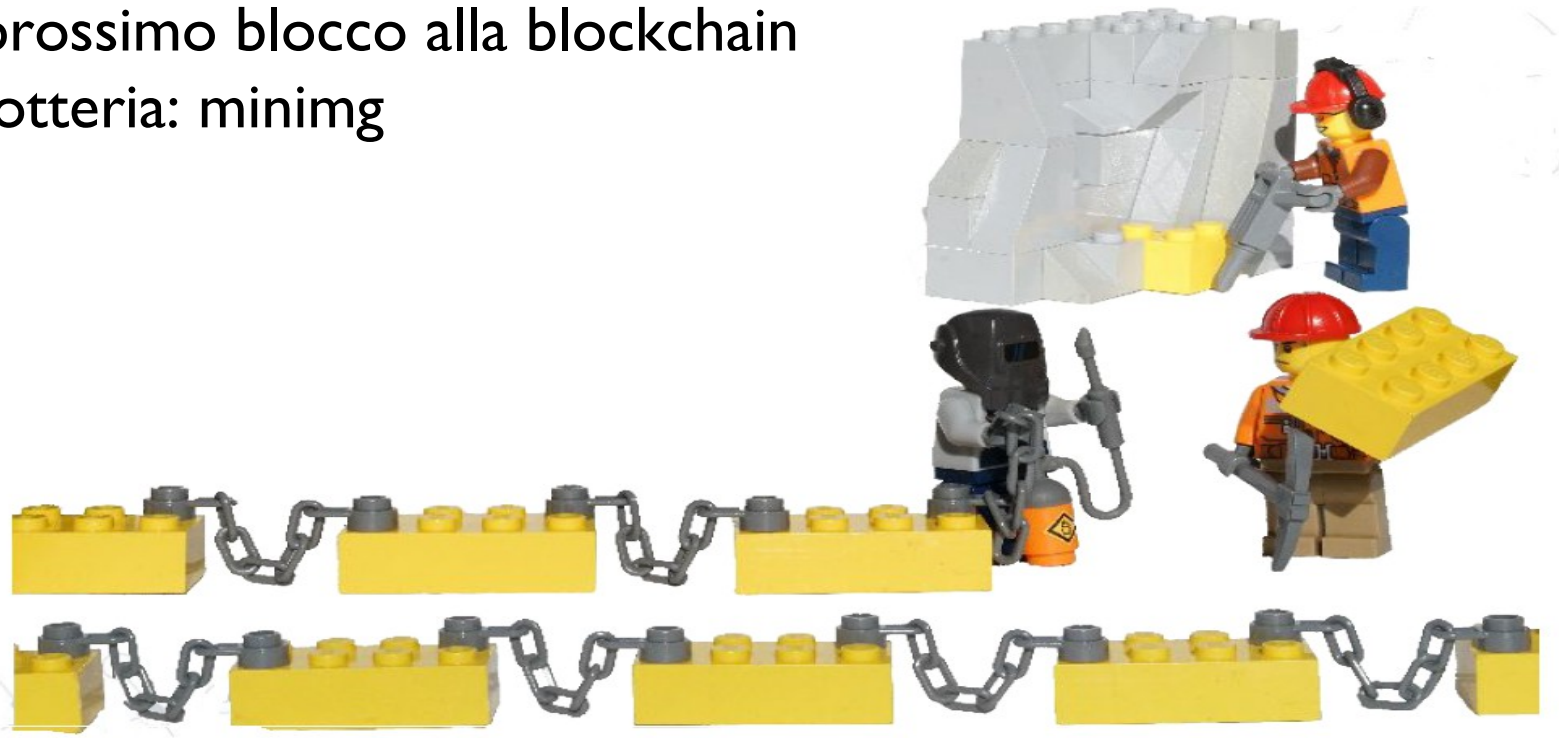
BLOCKCHAIN: IMMUTABILITA'

- se cambio il contenuto del blocco, devo ricalcolare gli hash di tutti I blocchi che lo seguono!
- modifico il 200.000-esimo blocco
  - cambia il suo hash
  - devo modificare l'hash del 201.000-esimo blocco
  - ….e così via: è necessario ricalcolare gli hash di tutti i blocchi che seguono il blocco 200.000, nella blockchain



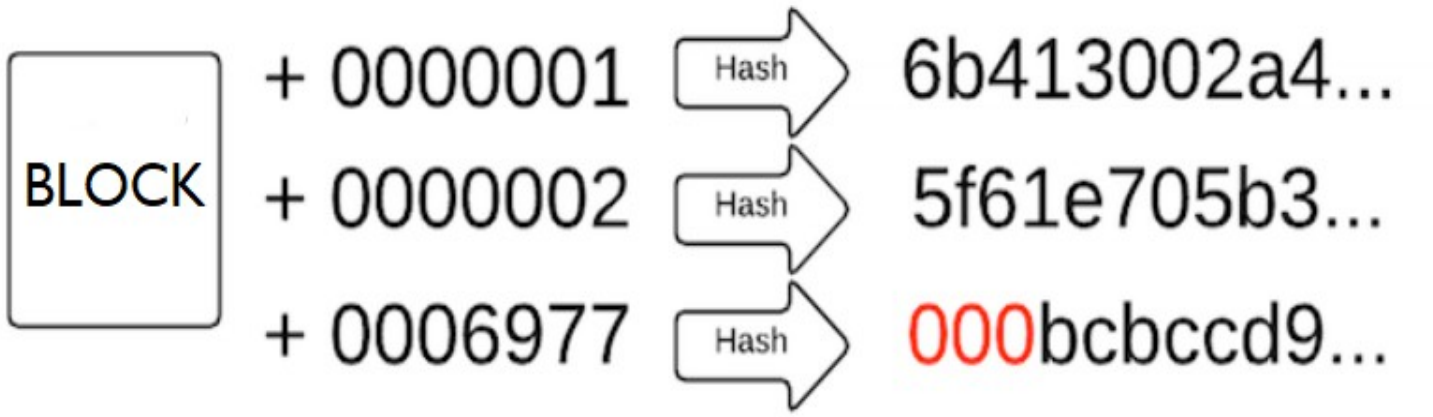
BITCOIN MINING

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



BLOCKCHAIN: PROOF OF WORK

- trovare un valore x tale che l'hash del blocco insieme ad x sia minore di un valore prefissato



- necessaria molta potenza computazionale anche per un singolo blocco

BLOCKCHAIN: PROOF OF WORK

- il processo di mining in Bitcoin costa troppo
  - largo spreco di energia
  - mining pools
- altre soluzioni attualmente proposte
  - proof of stake
  - blocco accettato se firmato da un certo insieme di partecipanti. Per ricreare la catena, necessario conoscere le chiavi private di tutti i partecipanti
  - Byzantine consensus

DISTRIBUTED LEDGERS OLTRE BITCOIN

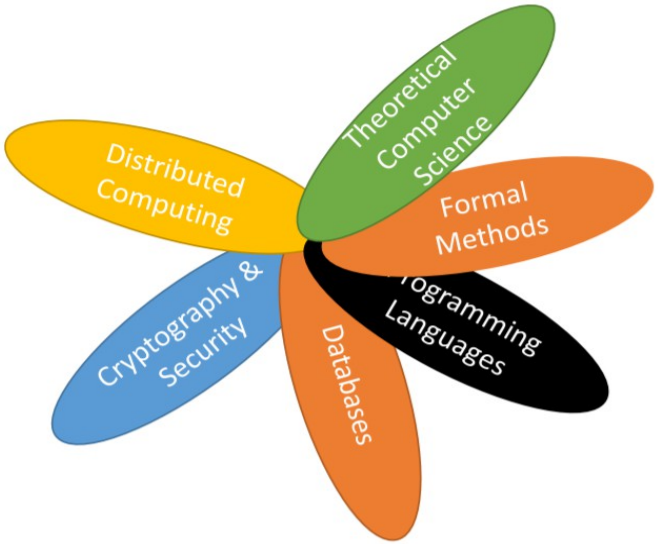
- Public vs Private Blockchain:
  - l'accesso è basato/non è basato su autenticazione (CHI sei?)
- Permission vs Permissionless Blockchain:
  - il ruolo da svolgere è basato/non è basato su autenticazione on user (COSA può fare un nodo).
- Blockchain Privata:
  - i nodi si connettono alla rete rispettando un insieme di regole (VPN, diritti, politiche, certificati digitali,..)
- Blockchain Permissioned:
  - il ruolo dei nodi è ristretto
  - alcuni partecipano al consenso, altri possono solo inserire transazioni, altri eseguono gli smart contracts
  - uno o più partecipanti hanno autorità di stabilire i ruoli

DISTRIBUTED LEDGERS: ESEMPI

- Public and Permissioned-less Blockchain: Bitcoin, Ethereum (PoW)
  - ogni nodo può entrare nella rete e partecipare al consenso
- Public and Permissioned Blockchain: Ripple, Stellar (PoS)
  - tutti possono partecipare alla rete, ma solo alcuni possono partecipare al consenso
- Private and Permissionless Blockchain: private Ethereum
  - i nodi possono unirsi alla rete solo se hanno credenziali/certificati per una VPN
  - ogni nodo può partecipare al consenso
- Private and Permissioned Blockchain: Hyperledger Fabric, Corda
  - la "privatezza" è garantita permettando ai nodi di unirsi al sistema solo se hanno diritti di accesso
  - il permesso di validare le transazioni (algoritmo di consenso) è attribuito solo a nodi specifici

CONCLUSIONI: HYPE OR 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:

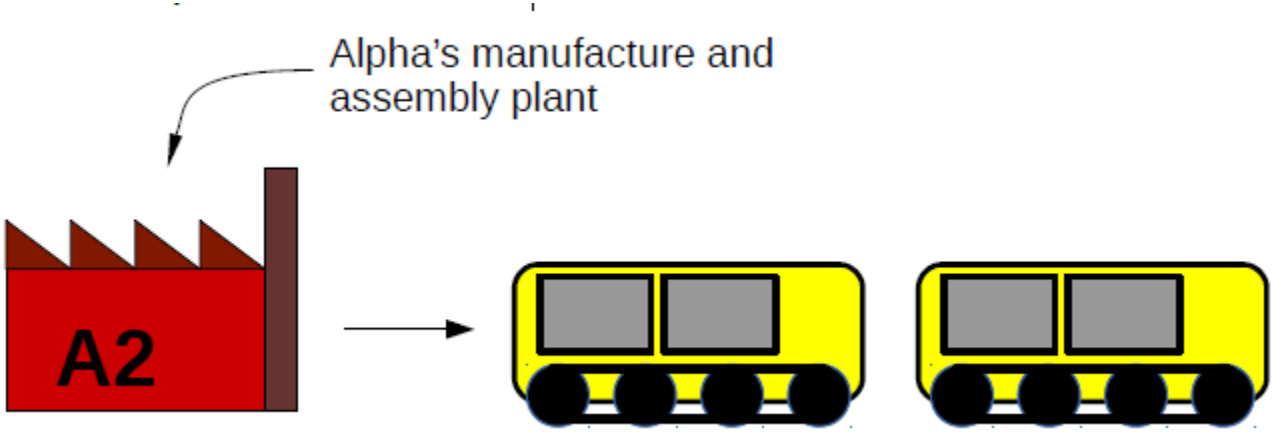
e le sfide tecniche sono complesse!

diverse aree della computer science sono coinvolte

A SUPPLY CHAIN SCENARIO

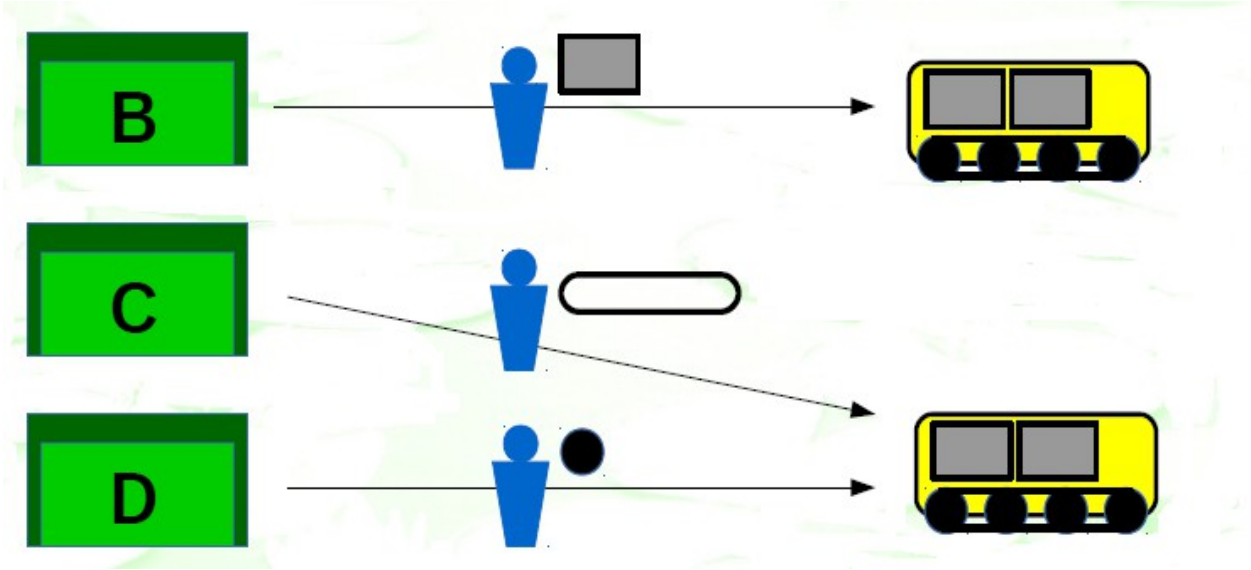
- Alpha corporation designs and oversees the manufacture of complex multi-part equipment, for example for heavy industry, A1 is Alphs's head office.

- the equipment ed in one of Alpha's factories, A2



A SUPPLY CHAIN SCENARIO

- the equipment is shipped to different remote locations and used heavily. Regular servicing and maintenance is required to comply with local safety rules and legislation.

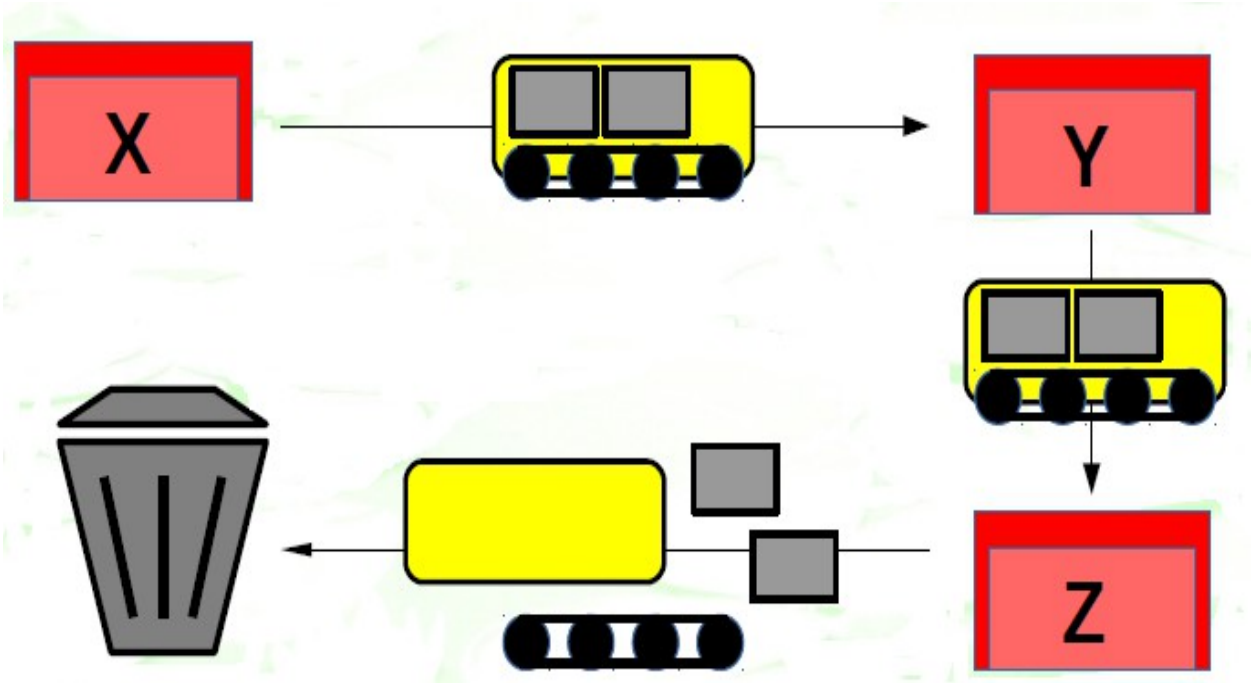


- Alpha contracts out equipment maintenance to authorized third parties, who use certified service engineers and approved replacement parts

A SUPPLY CHAIN SCENARIO

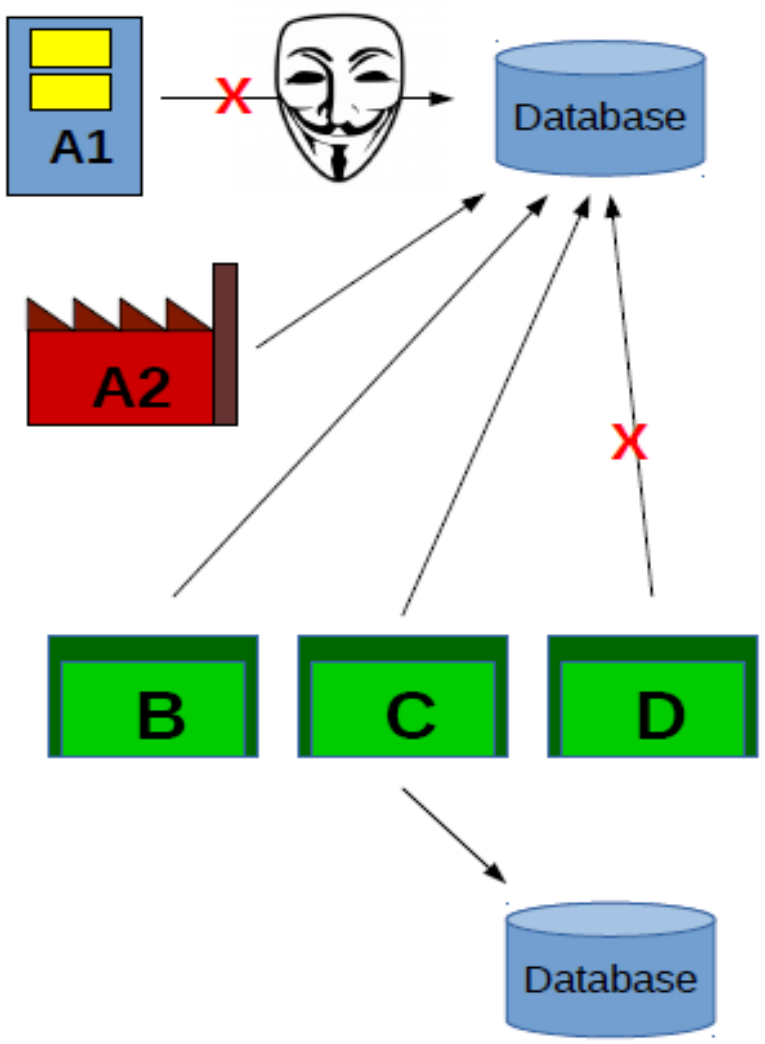
The scenario

- equipment may be sold from one corporation to another, and a record of the service history and provenance is vital
- at the end of the life-cycle the equipment is decommissioned



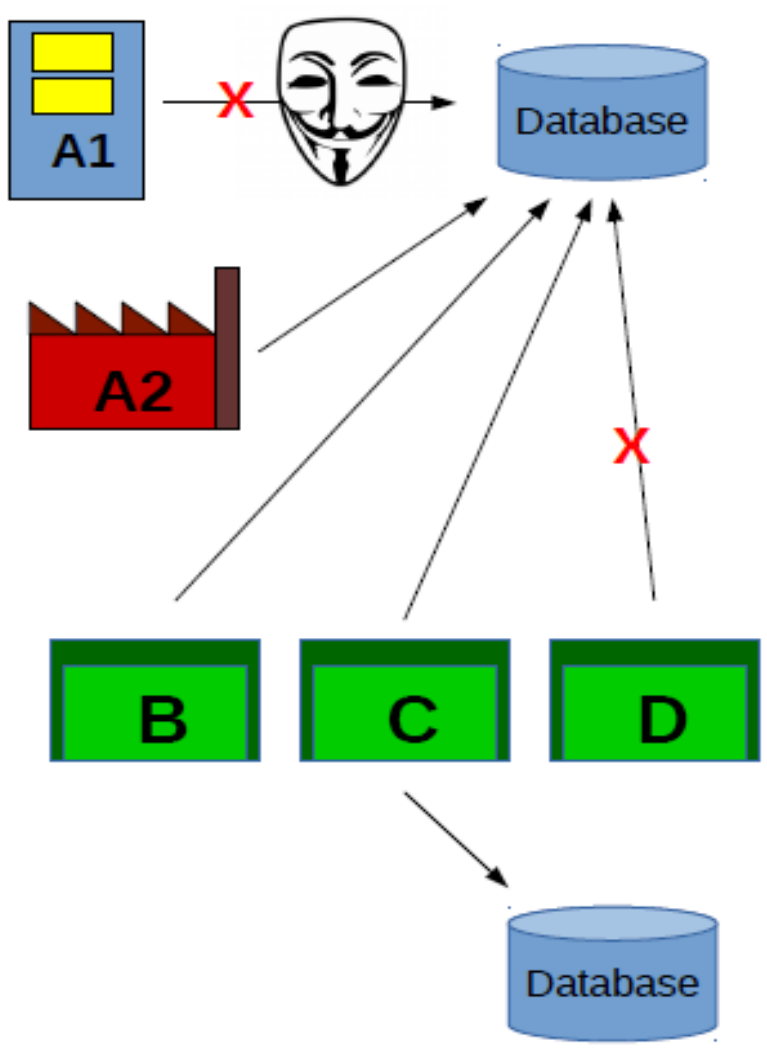
A SUPPLY CHAIN SCENARIO

- A1 runs a centralized database to track
  - Components
  - Equipments
  - Locations
  - service histories and life-cycle.
- a denial of service attack on a database (or even database server farm) may result in a serious risk
  - records in any databases can be altered or deleted
- some processes such as replacement part orders are manual, requiring human memory and intervention.



A SUPPLY CHAIN SCENARIO

- sharing access to the databases may be limited or be blocked by participants at any time without notice.
- problems to be faced:
  - compliance and third-party auditing
  - access permission granting and revocation
  - interoperability between different systems
- disputes can be difficult to solve at a later date
  - costly and protracted legal action.



A SUPPLY CHAIN EXPLOITING BLOCKCHAIN

Component tracking and servicing on a blockchain has several adavantages

- blockchains are distributed: distinct nodes in several locations run the software powering the blockchain and keep a copy of the data. More nodes implies:
  - more backup copies of the data
  - more backup "servers"
  - denial of service attacks become impossible
- blockchains are tamper-proof: as soon as a record is inserted into a blockchain, it is locked down, and cannot be changed.
  - hacking the data records becomes impossible
  - "delete and deny" defenses become impossible
  - auditing: a simple scan over the blockchain

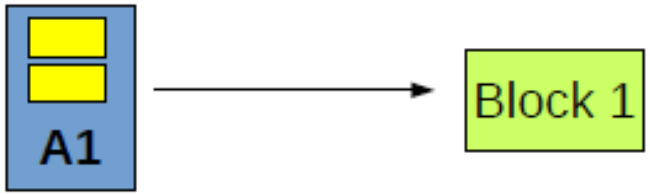
A SUPPLY CHAIN EXPLOITING BLOCKCHAIN

component tracking and servicing on a blockchain has several adavantages:

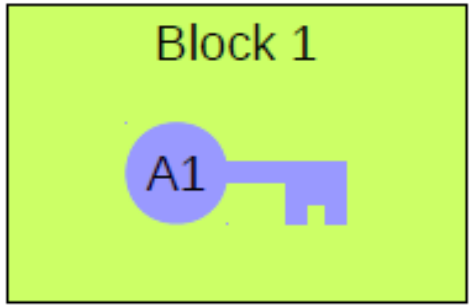
- blockchains can support "smart contracts"
  - components have their required service and replacement history pre-loaded onto the blockchain using a "smart contract"
  - when the scheduled service date or wear-and-tear usage limit is reached, the system automatically triggers a service request
  - on completion of the service or replacement, a record is generated on the blockchain

A SUPPLY CHAIN EXPLOITING BLOCKCHAIN

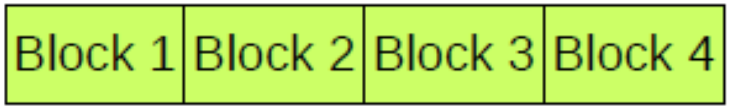
- the Alpha company:
  - starts a "permissioned blockchain" with a "genesis block"
  - runs the first block on the chain on a computer in its head office



- the genesis block contains the announcement message of Alpha's first public key
  - this key will identify Alpha head office on the blockchain in future.

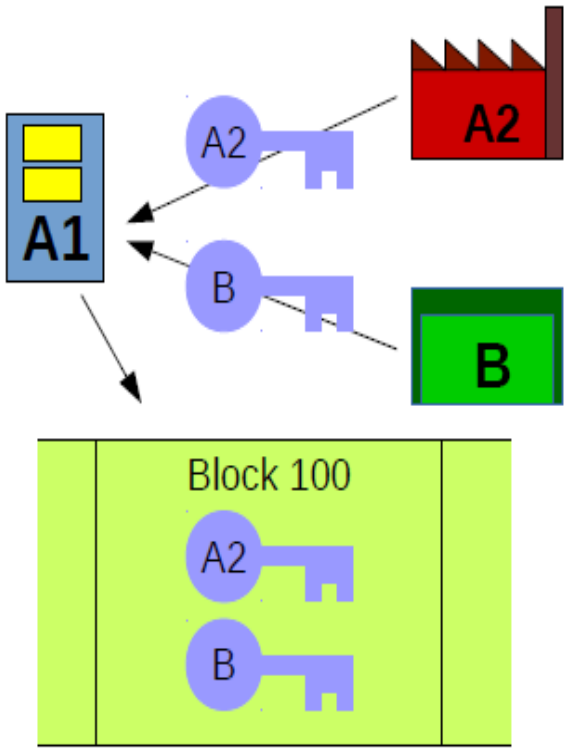


- the blockchain runs, and at regular intervals new blocks are added by Alpha's blockchain node.



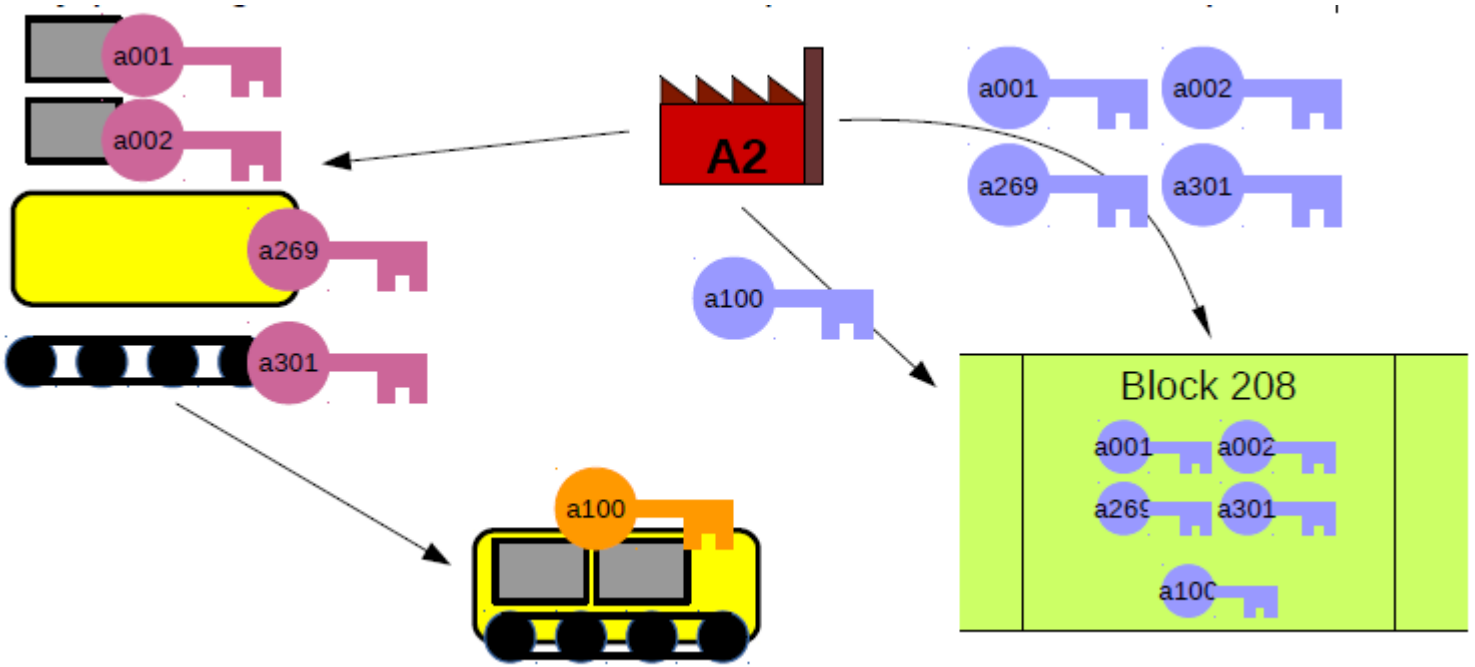
A SUPPLY CHAIN EXPLOITING BLOCKCHAIN

- Alpha's factory A2 and the contracted service company B
  - generate public/private key pairs
  - send the public keys to A1, who announces it on the blockchain
- now A2 and B join the blockchain
  - run their own blockchain nodes
  - add blocks onto the blockchain
  - are nodes in the blockchain P2P network
- A1 does not know A2 and B's associated private keys and they don't A1's private key
  - no one of the participants can impersonate each other
  - a message on the blockchain signed with B's private key and verified with its public key is verified to come from B.

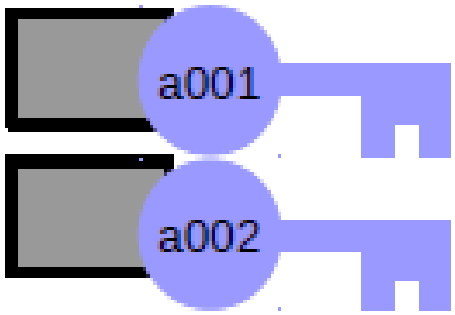


A SUPPLY CHAIN EXPLOITING BLOCKCHAIN

- A2 which manufactures components
  - creates a unique private/public key pair for each component
  - announces the public key on the blockchain, along with the location of the part, which is its factory warehouse.
- the components are assembled to produce the final machine
  - another key pair is generated for the finished product and is also reported



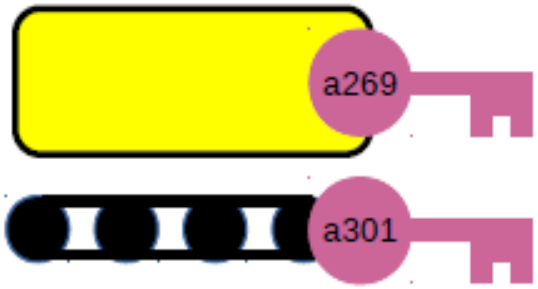
A SUPPLY CHAIN EXPLOITING BLOCKCHAIN



cheap components: marked with a QR code of the public key for scanning,

- do not participate to the blockchain
- other RFID scanning devices read the key value and submit reports to the blockchain on their behalf.

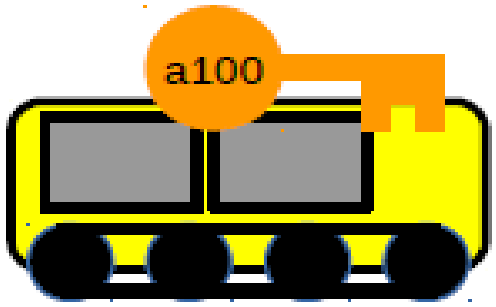
A SUPPLY CHAIN EXPLOITING BLOCKCHAIN



more expensive components:

- marked with an active RFID tag with Bluetooth connectivity.
- can contact nearby network connected devices and submit reports to the blockchain,

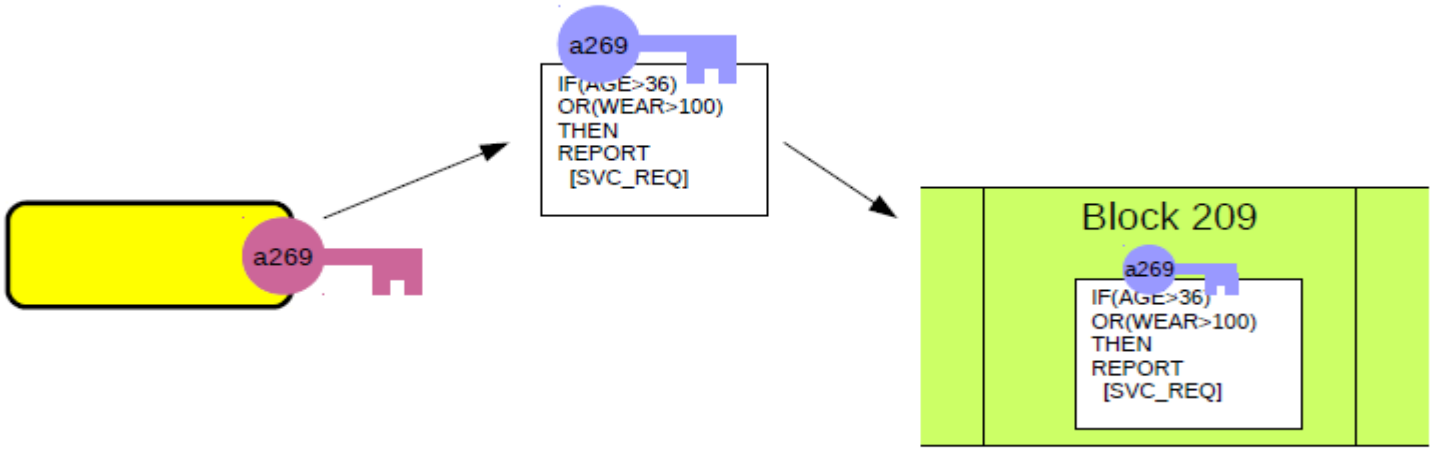
A SUPPLY CHAIN EXPLOITING BLOCKCHAIN



- finished machinery may have
  - a fully connected IoT device, with good connectivity to the network
  - onboard GPS for positionin
  - possibly a lightweight blockchain node for participating in the generation of new blocks.
- an integrated RFID tag reader
  - scans the complete machine for all its components,
  - detects changes made to those components.

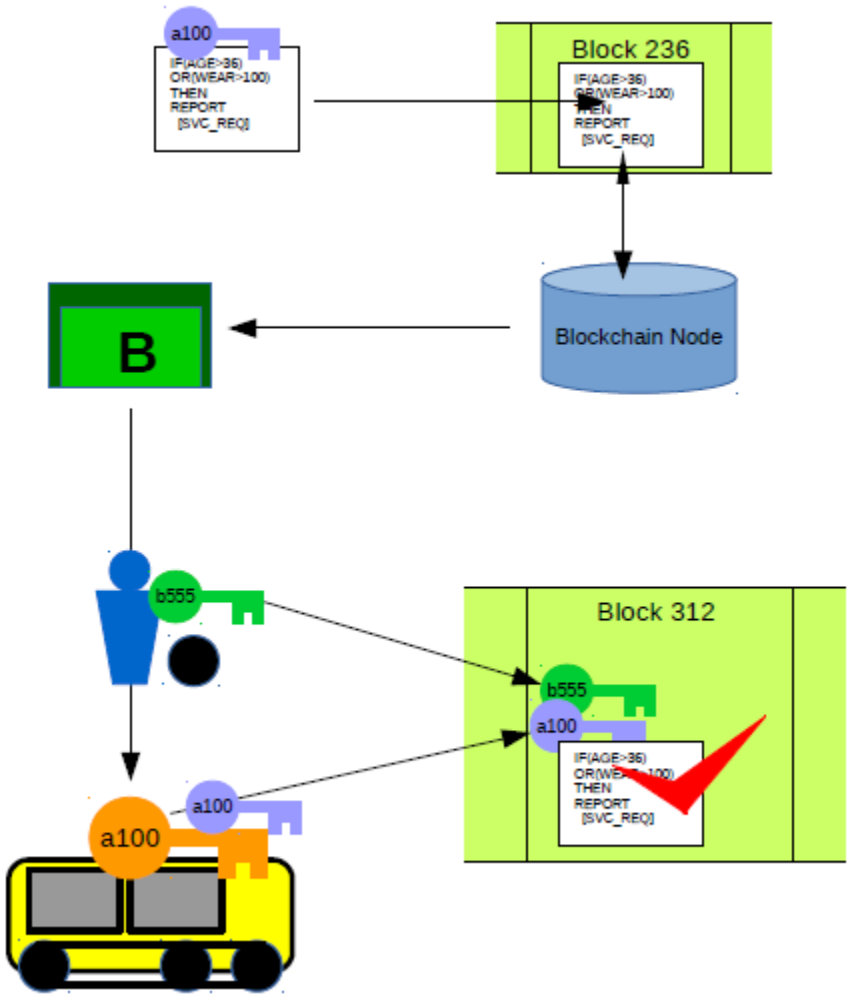
A SUPPLY CHAIN EXPLOITING BLOCKCHAINS

- when a component is logged on the blockchain by its public key announcement, a "smart contract" can be attached to the announcement
- this script will be run by nodes maintaining the blockchain if certain conditions are met.
- such contracts can trigger a service request, decommissioning, or part replacement order to automatically be sent to a service engineering company.
- the complexity of the automation provided depends on the design of the blockchain system.



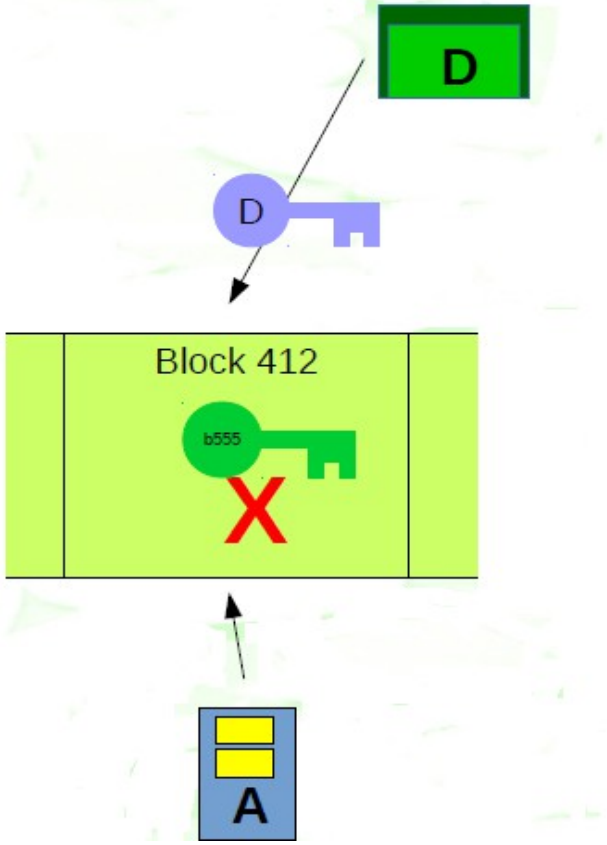
A SUPPLY CHAIN EXPLOITING BLOCKCHAINS

- A condition of the smart contract is met, a node generating the current block sends out a service request to B
- B sends a service engineer to the machinery in order to replace the wornout part.
- Service engineers are certified on the blockchain by their own private/public key, stored in their smartphone or their service tablet
- the engineer replaces the part, the tablet and the machine's central IoT device may send reports back to the blockchain to record the event. The contract is met.



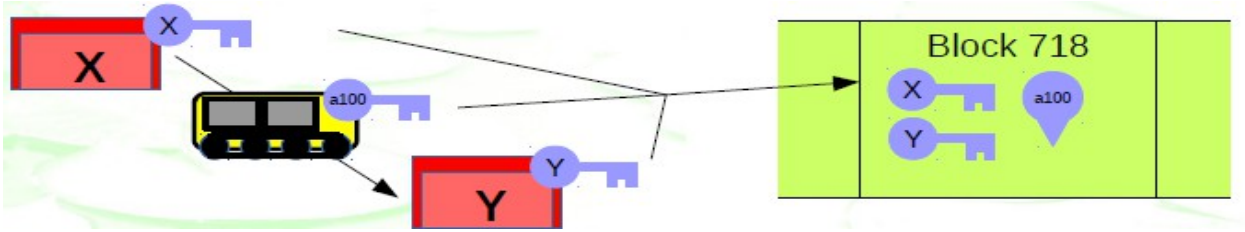
A SUPPLY CHAIN EXPLOITING BLOCKCHAINS

- D decides to revoke a service engineer's certification: he/she lefts the company...
- D posts
  - a key revocation message on the block chain
  - signed with his/her private key, revoking key b555.
- D can do this because he/she issued and signed the key in the first place.
- all records made with key b555 prior to block 412 remain valid, however, and the records cannot be removed.

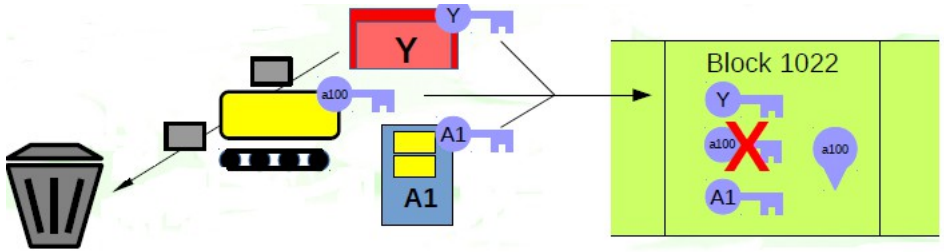


A SUPPLY CHAIN EXPLOITING BLOCKCHAINS

- company X is the owner of the machine, and sells it to company Y.
  - the record of ownership and the location change of the machine is recorded to the blockchain
  - it provides a future immutable record of its provenance.



- at the end of the life-cycle the equipment is decommissioned,
  - this event is recorded on the blockchain, with a signature from the original manufacturer, A.
  - this allows future trusted auditing of the application of environmental legislation to be conducted.



A SUPPLY CHAIN EXPLOITING BLOCKCHAINS

At the end of the process a complete record exists on the blockchain of all:

- participants
- components
- their locations and journeys, who replaced what parts and where and when
- transfer of ownership
- final decommissioning

The records cannot be altered or deleted afterwards

- individual participants can track progress during transit, and review the data after delivery, alteration or transfer
- only those directly concerned with or involved in the design, manufacture, repair or order fulfillment can create relevant records
- there is no central server or central point of failure