ALL'INTERNO DELLA BLOCKCHAIN

Ing. Giuseppe Spera
Data Protection Officer
Ordine degli Ingegneri della Provincia di Caserta

Cos'è Blockchain

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

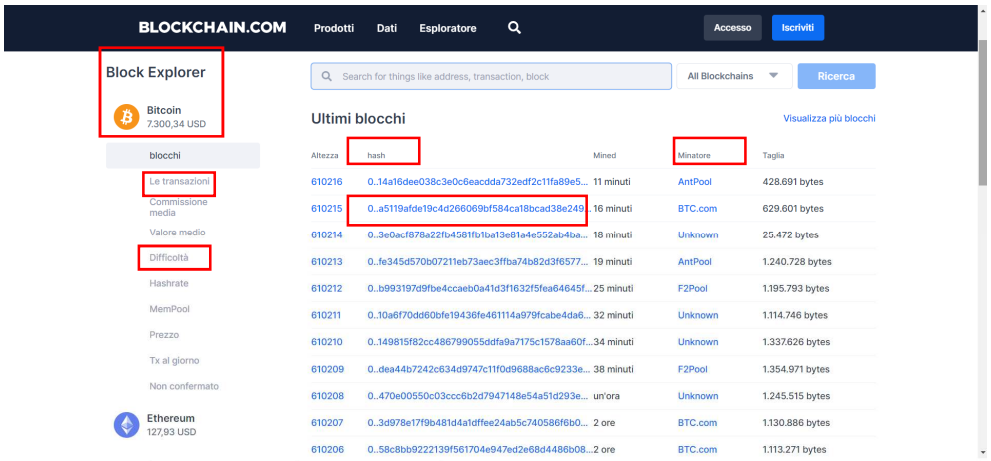
«Un ***registro*** digitale le cui voci sono raggruppate in ***blocchi***, ***concatenati*** in ***ordine cronologico***, e la cui ***integrità*** è garantita dall'uso della ***criptografia***.» Wikipedia.org

È un ***sistema distribuito*** in cui è possibile ***memorizzare*** in maniera permanente qualsiasi tipo di elemento, ***senza la necessità di un'autorità centrale fidata***.

Esistono diverse piattaforme che operano secondo il modello della Blockchain: Bitcoin, Ethereum, Corda, Hyperledger.

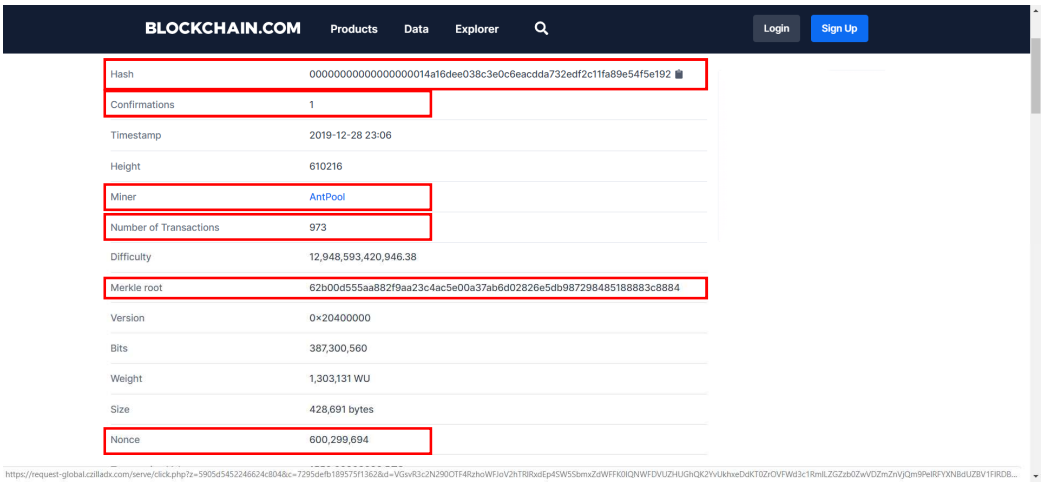
Perché….all'interno della blockchain

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA



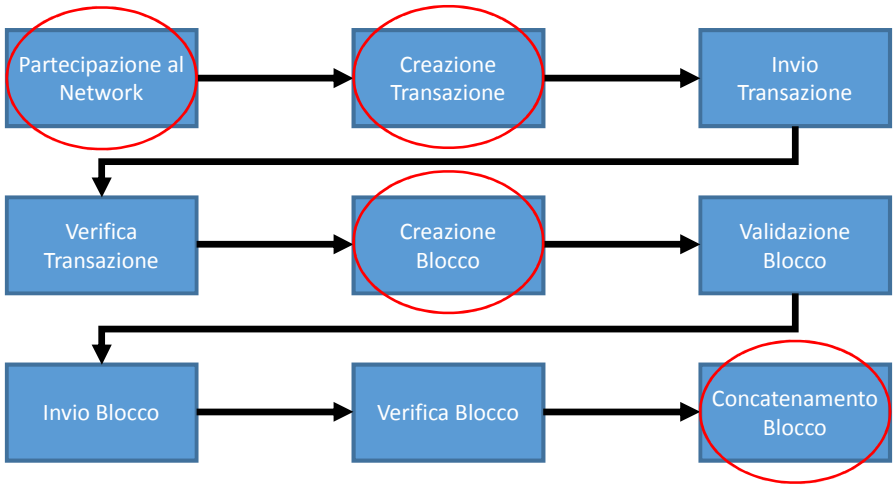
Perché….all'interno della blockchain

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA



Il processo che descrive la Blockchain

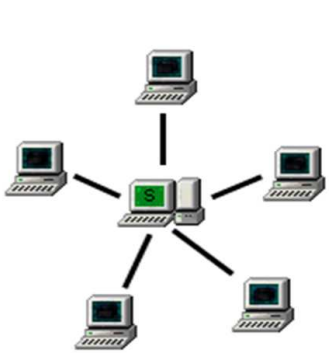
ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA



Partecipazione al Network

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

I partecipanti alla Blockchain sono un gruppo di computer o in generale di device che fanno parte di un network. Questi device sono definiti «nodi».

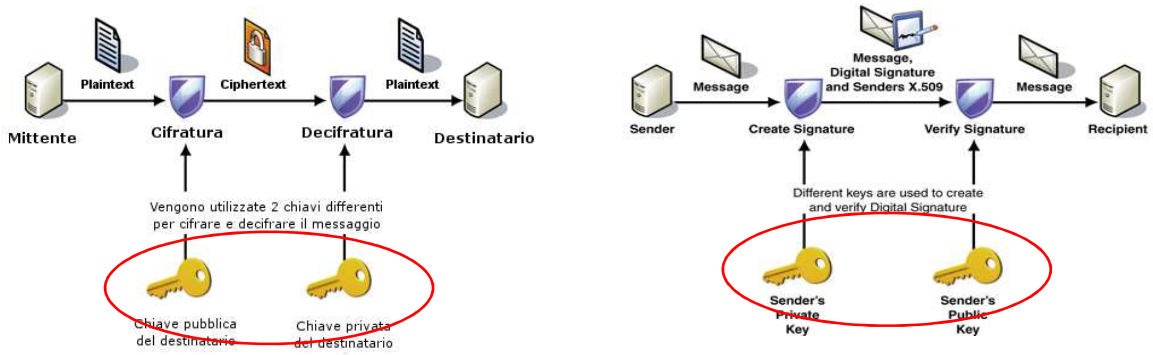


Sistema Centralizzato

Sistema Distribuito

Crittografia a chiave asimmetrica

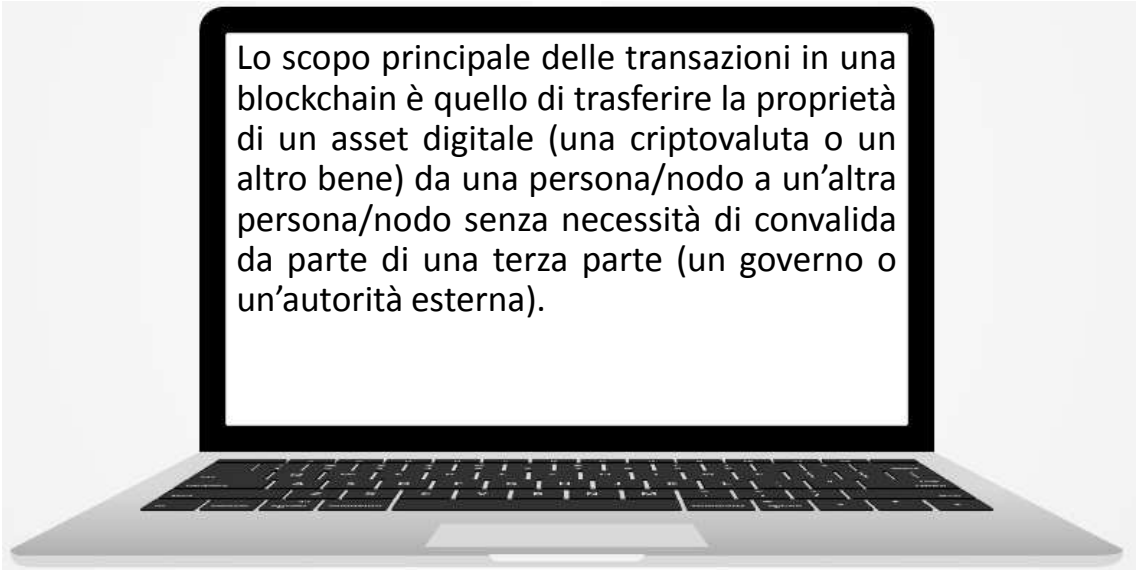
ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA



Ogni nodo del Network possiede una coppia di chiavi crittografiche.
«Public Key» e «Private Key»

La transazione in una blockchain

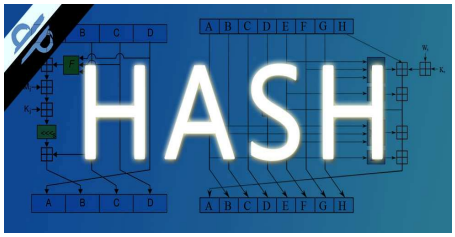
ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

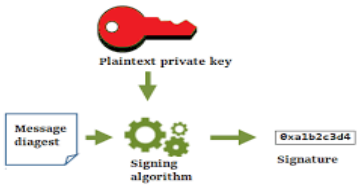


Creare una transazione sulla Blockchain

Transazione n-esima con n = 1

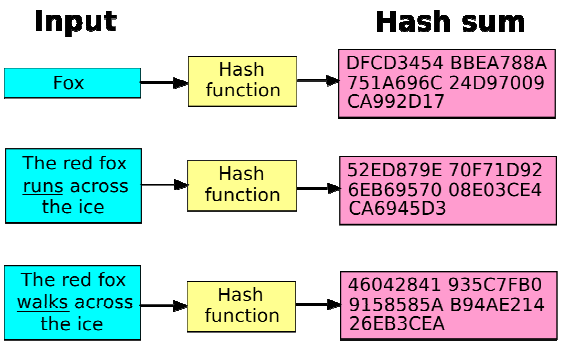
Transaction Hash della transazione n = 0	DigitalAsset che si vuole trasferire	Dati Opzionali della transazione	PublicKey del destinatario «Address»	Transaction Hash della transazione n = 1	Signature del mittente



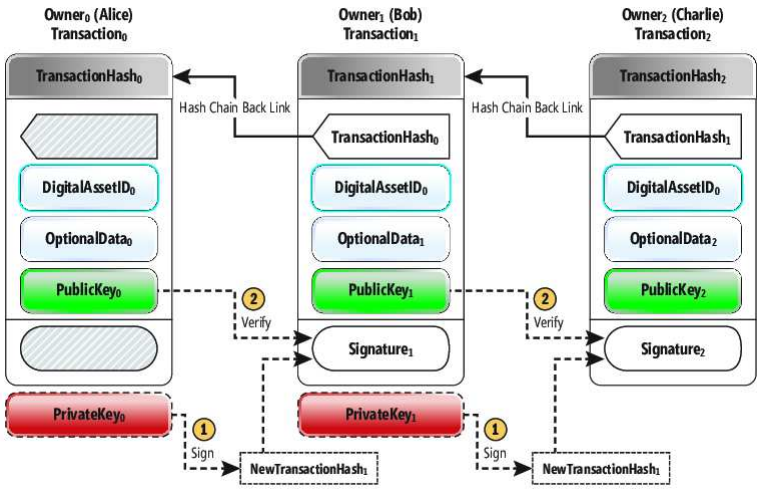


Funzione di HASH

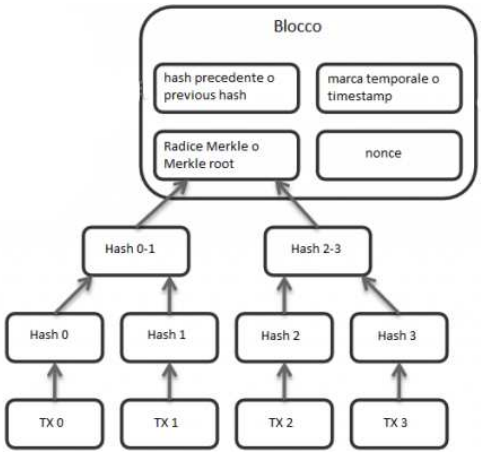
Si tratta di un algoritmo matematico che mappa dei dati di lunghezza arbitraria (*messaggio*) in una stringa binaria di dimensione fissa chiamata *valore di hash*. Tale funzione di hash è progettata per essere unidirezionale (*one-way*). La funzione deve identificare univocamente il messaggio, non è possibile che due messaggi differenti, pur essendo simili, abbiano lo stesso valore di hash e deve essere deterministico, in modo che lo stesso messaggio si traduca sempre nello stesso hash.



Creare una catena di transazioni sulla Blockchain



Creazione del Blocco



Previous Hash
- Valore di Hash del blocco precedente

Timestamp
- Marca Temporale

Merkle Root
- La radice Merkle è una rappresentazione ridotta del set delle transazioni che vengono confermate con questo blocco

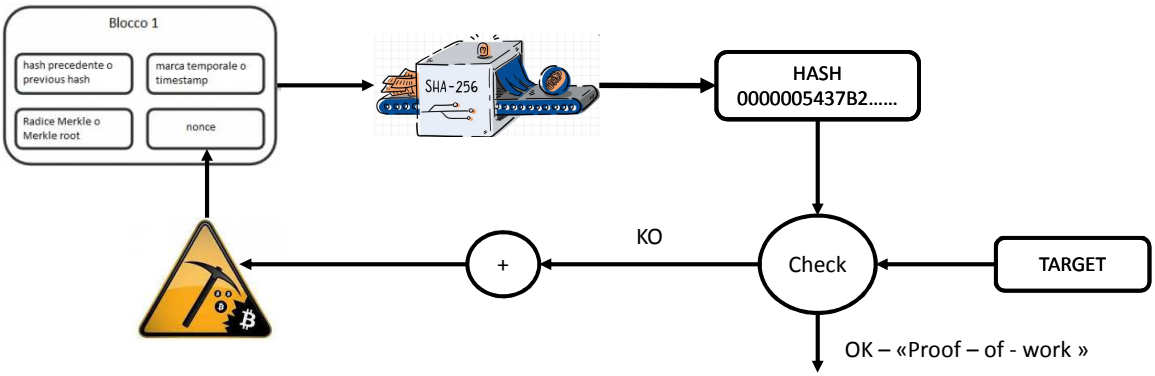
Proof of work / Nonce
- Numero arbitrario di 4 byte che permette di generare un Hash del blocco composto inizialmente da una stringa di zeri di lunghezza l fissata dalla rete

Validazione del Blocco - 1

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

Proof – of – work

La proof-of-work (PoW) è il metodo con cui un miner certifica, tramite la risoluzione di un algoritmo matematico, la validazione di un blocco di transazioni, trovando per ciascun nuovo blocco di transazioni un nonce (un numero casuale usato una sola volta) da includere nei dati di input



Validazione del Blocco - 2

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

Un semplice esempio:

- Usiamo la stringa "Hello, world!" come dato di input della funzione di HASH, si ottiene un «hash value» deterministico che inizia con 315F;
- Supponiamo ad esempio che come «TARGET del Network» si richiede di fare iniziare l'hash value con 0000, si dovranno effettuare migliaia di tentativi prima di trovare una soluzione;

→ SHA-256("Hello, world!")= 315F5BDB76D078C43B8AC0064E4A0164612B1FCE77C869345BFC94C75894EDD3

→ SHA-256("Hello, world!0")= 1312AF178C253F84028D480A6ADC1E25E81CAA44C749EC81976192E2EC934C64

→ SHA-256("Hello, world!1")= E9AFC424B79E4F6AB42D99C81156D3A17228D6E1EEF4139BE78E948A9332A7D8

.....

→ SHA-256("Hello, world!4249")= C004190B822F1669CAC8DC37E761CB73652E7832FB814565702245CF26EBB9E6

→ SHA-256("Hello, world!4250")= 0000C3AF42FC31103F1FDC0151FA747FF87349A4714DF7CC52EA464E12DCD4E9

Ovviamente, i miner vengono remunerati per svolgere questo processo di verifica, di conseguenza, questi competono fra loro per risolvere il blocco, in quanto il primo che lo risolve otterrà una ricompensa.
Il processo di mining o proof – of- work richiede un elevato dispendio di potenza di calcolo e risorse energetiche.

Verifica del Blocco

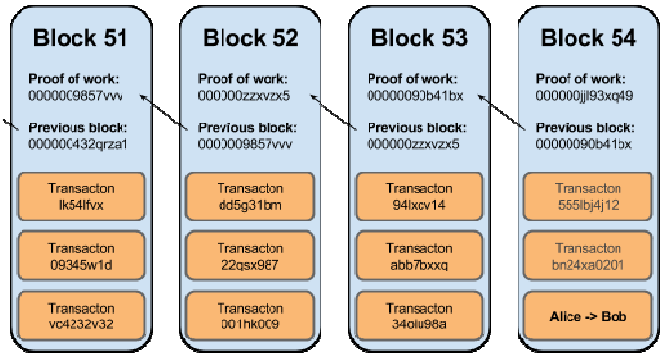
ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

Una volta determinato il valore di hash che valida il blocco, questo viene trasmesso a tutti i nodi della rete che ne verificano la validità.

Il blocco è convalidato dai nodi della rete

Concatenamento della BlockChain

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA



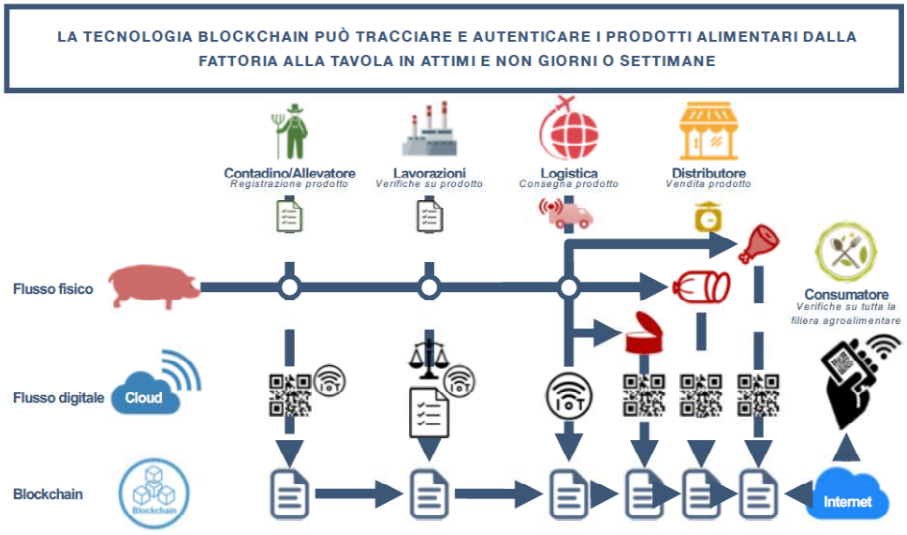
Possibili ambiti di applicazioni

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

Scuola e Università	Certificazione Titoli e certificati accademici
Voto	Certificazione del monitoraggio e del conteggio dei voti
Automotive	Concessione in leasing di un'auto in modo autonomo Noleggio autovetture
Manutenzioni	Certificazione delle attività di manutenzione
Musica	Gestione dei diritti d'autore tramite pagamenti diretti agli artisti e utilizzo di smart contract
Beneficienza	Certificazione e tracciamento delle donazioni
Immobiliare	Automazione degli affitti tramite smart contract e iot
Immobiliare	Certificazione di registrazioni, monitoraggio e trasferimenti titoli fondiari, atti di proprietà
Assicurazioni	Polizze assicurative istantanee Assicurazioni P2P
Sanità	Registrazione e condivisione della cartella clinica
Supply Chain	Certificazione dei passaggi di una filiera produttiva
Armi	Monitoraggio della compravendita di armi
HR	Certificazione della veridicità delle Precedenti esperienze lavorative e verifica dei curriculum
Telco	Invio di messaggi certificati tra dispositivi iot che garantiscono integrità delle informazioni

Possibili ambiti di applicazioni

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA



Simulatore Blockchain

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

- http://blockchain.mit.edu/how-blockchain-works

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

Ing. Giuseppe Spera

Data Protection Officer

Ordine degli Ingegneri della Provincia di Caserta