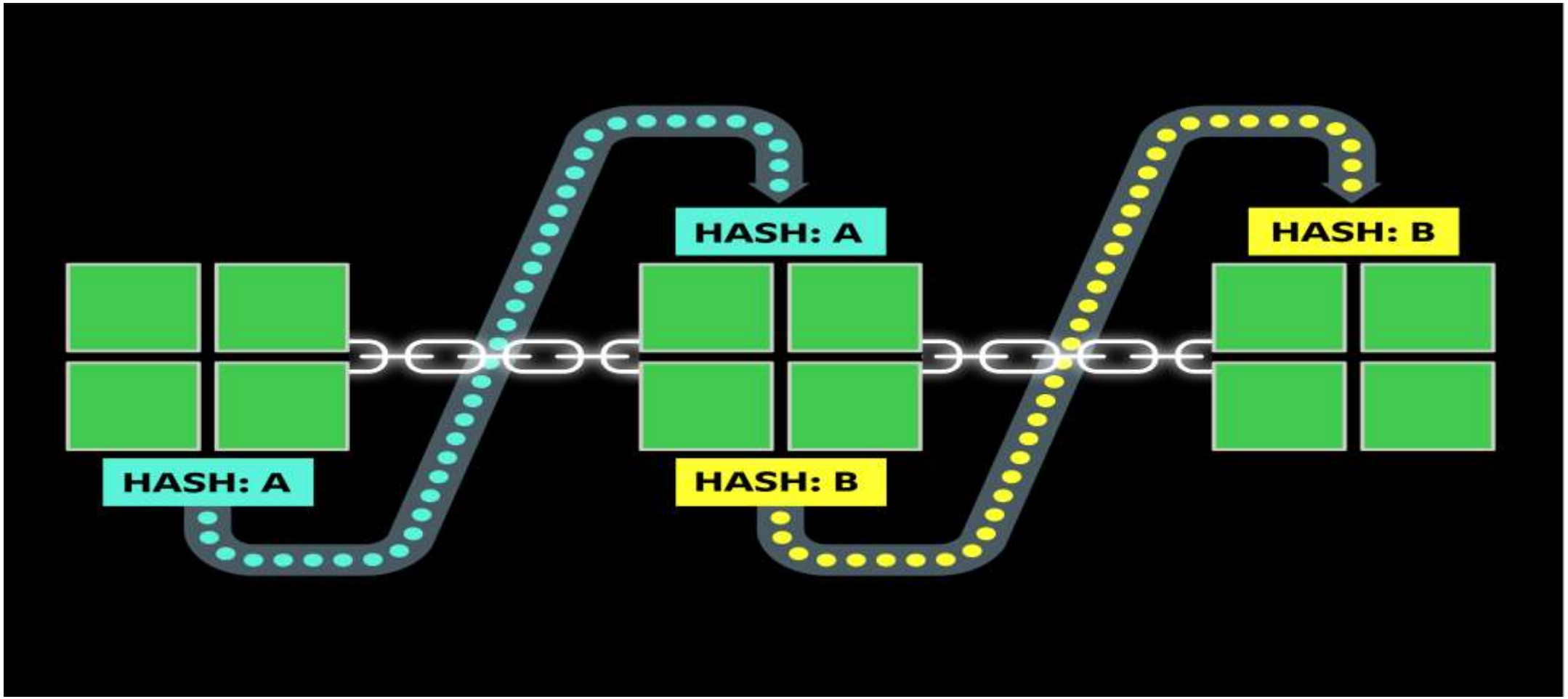
Cos'è la blockchain?

È un elenco collegato unidirezionale (Singly linked list). dove ogni blocco si riferisce al blocco precedente. Per questo, ogni nuovo blocco calcola l'hash(SHA256) del blocco precedente e lo inserisce nella sua intestazione. In questo modo ci assicuriamo che le informazioni all'interno di ciascun blocco non siano cambiate.



Perché la blockchain è importante?

In effetti, la blockchain in sé non è molto importante!
Importante è piuttosto l'algoritmo che decide chi ha il diritto di aggiungere un nuovo blocco alla lista.

Prima dell'algoritmo **PoW**, che spiegherò un po' più avanti, l'unico modo per ottenere consenso, accordo e prendere decisioni era votare. Cioè, il gruppo a cui è stato permesso di votare per qualsiasi motivo si è consultato e ha raggiunto la decisione finale votando.
Naturalmente, a volte solo una persona poteva prendere decisioni, cosa che oggi chiamiamo **dittatura**.

Ma cos’è il PoW?

Per spiegare questo algoritmo, dobbiamo conoscere un po’ la crittografia. In questo momento spiegherò la funzione hash e successivamente parlerò della crittografia asimmetrica.

256 bits = 32 bytes

Hello world!

2cf24dba5fb0a30e11c6f83451d25e1f1752e4
b7e0443e2725515d0d3e21c0010

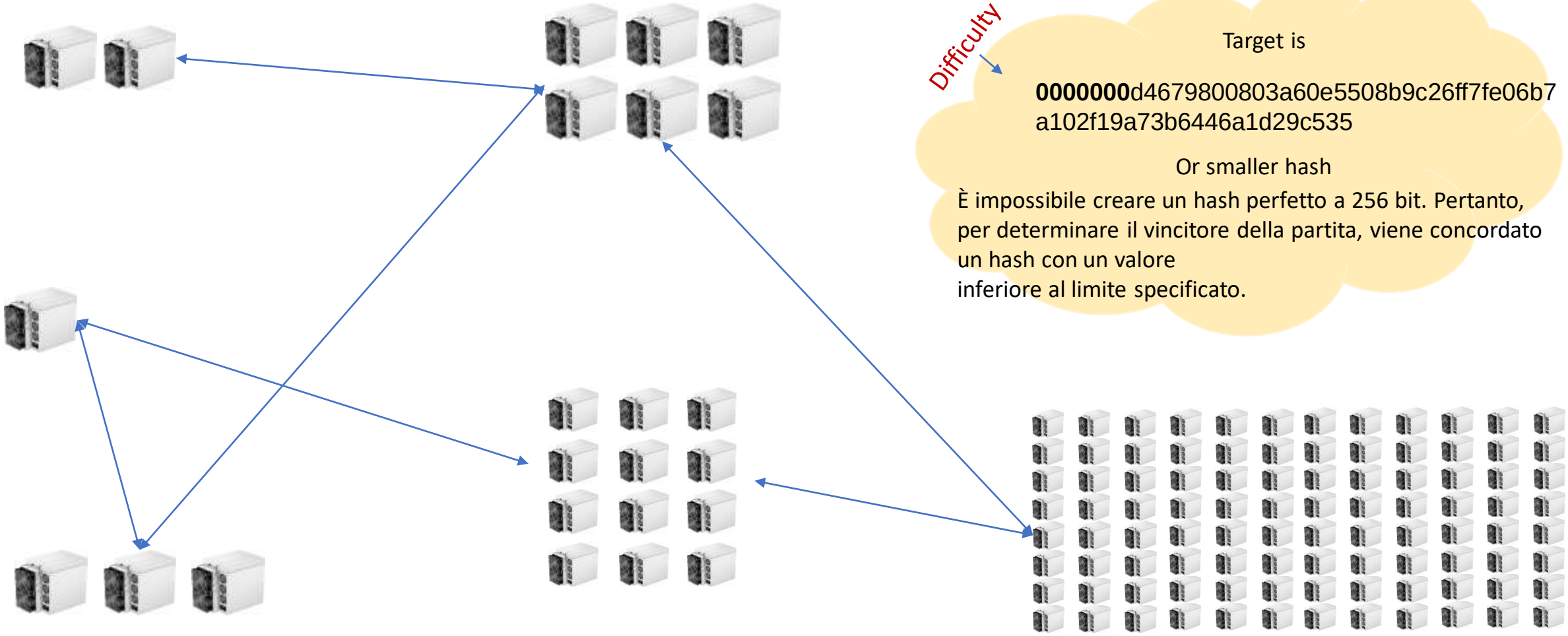
f7fe06b7a102f19a73b6446a1d29c535887ad7
0d5d49800803a60e5508b9c26f

000ad70d5d49800803a60e5508b9c26ff7fe06
b7a102f19a73b6446a1d29c535

Un algoritmo hash è una funzione matematica che accetta un input di qualsiasi dimensione, ad esempio una stringa di testo, un'immagine o un file, e produce un output di dimensione fissa chiamato valore hash. Il valore hash è come un'impronta digitale dei dati di input.

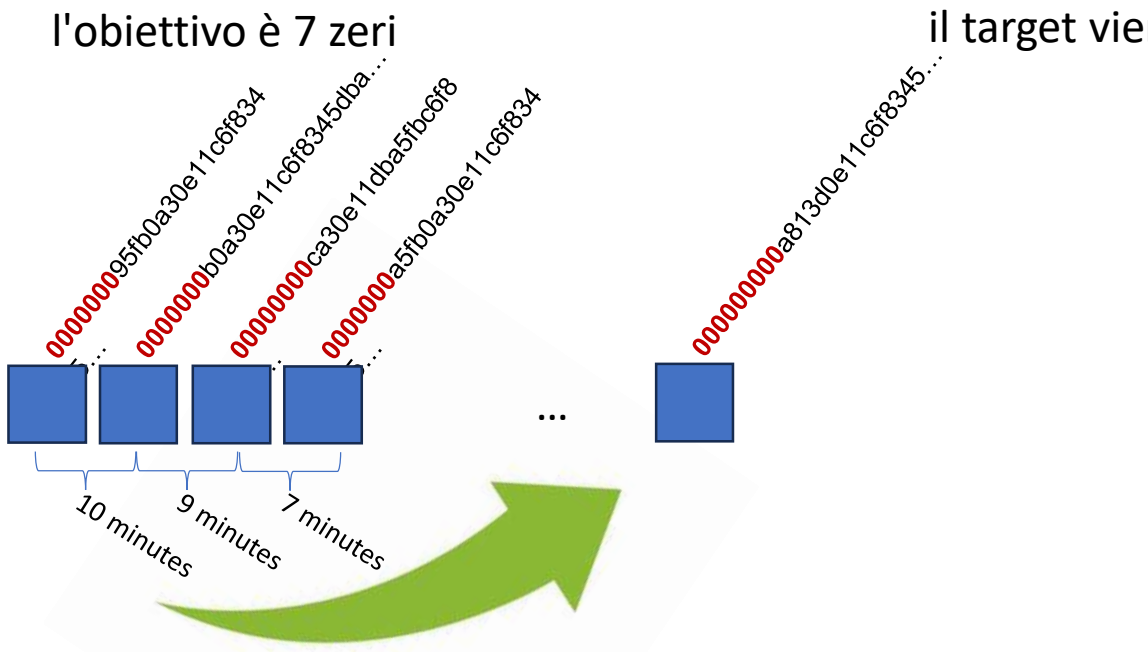
Tenete presente che questo algoritmo è unidirezionale ed è impossibile sapere cosa viene sottoposto a hash conoscendo il valore hash. E non è possibile prevedere l'output modificando il input.

Pertanto, l'unico modo per produrre un output specifico è modificare l'input, eseguire l'hashing e calcolare l'output finché non viene prodotto quell'output specifico.
Significa milioni (e anche miliardi di miliardi) di volte di tentativi ed errori! **Proof of Working**



Difficulty auto adjustment

Quale era il genio di **Satoshi Nakamoto** (Inventore del Bitcoin)?
Regolazione automatica della cifre di difficoltà!
Il valore di difficoltà (o il numero di zeri) è sempre impostato in modo che siano necessari circa dieci minuti per trovare un hash adatto.



più macchine o
macchine più potenti collegate alla rete

E come vengono prese le decisioni adesso?

Una persona prende una decisione e gli altri ne controllano la correttezza. E quella persona è stata trovata casualmente (PoW).

Una soluzione per aver organizzazioni
decentralizzate
e senza testa, inarrestabili
e Incensurabile.

Bitcoin motto:

Do not trust! Verify!

Ma cosa si controlla?
Ogni macchina (nodo), prima di tutto, controlla il hash della blocco se l'hash stesso è corretto e se ha soddisfatto il valore di difficoltà.

Successivamente, controlla il contenuto del blocco.

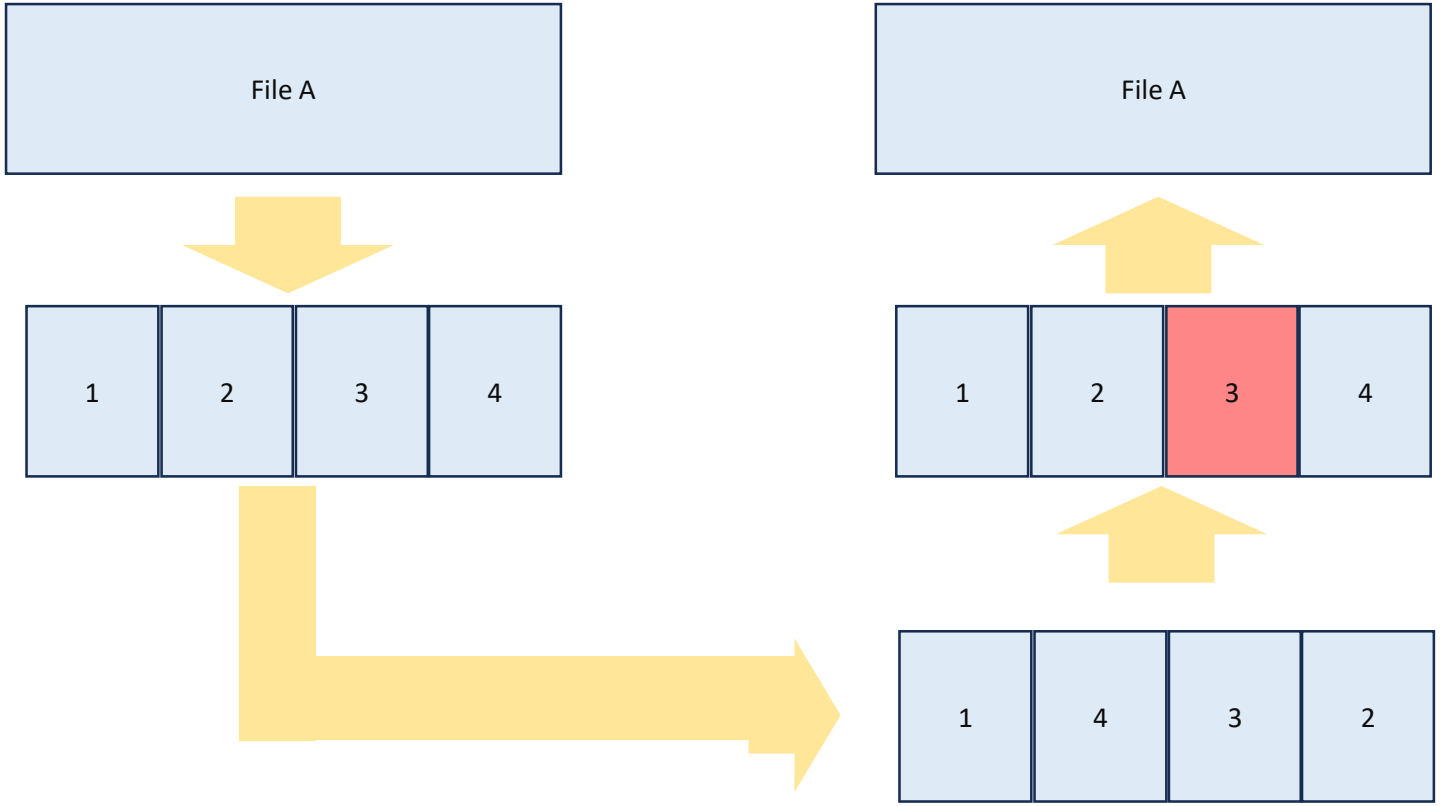
- Quali sono il contenuto del blocco?

- - header (link to previous block)
- - timestamp (block creation date and time)
- - nonce (a random number which is used to change the block hash)
- - transactions
- - transactions **Merkle** root hash
- - …

block hash (hash of entire block). This hash will be used in next block as reference to its prevous block.

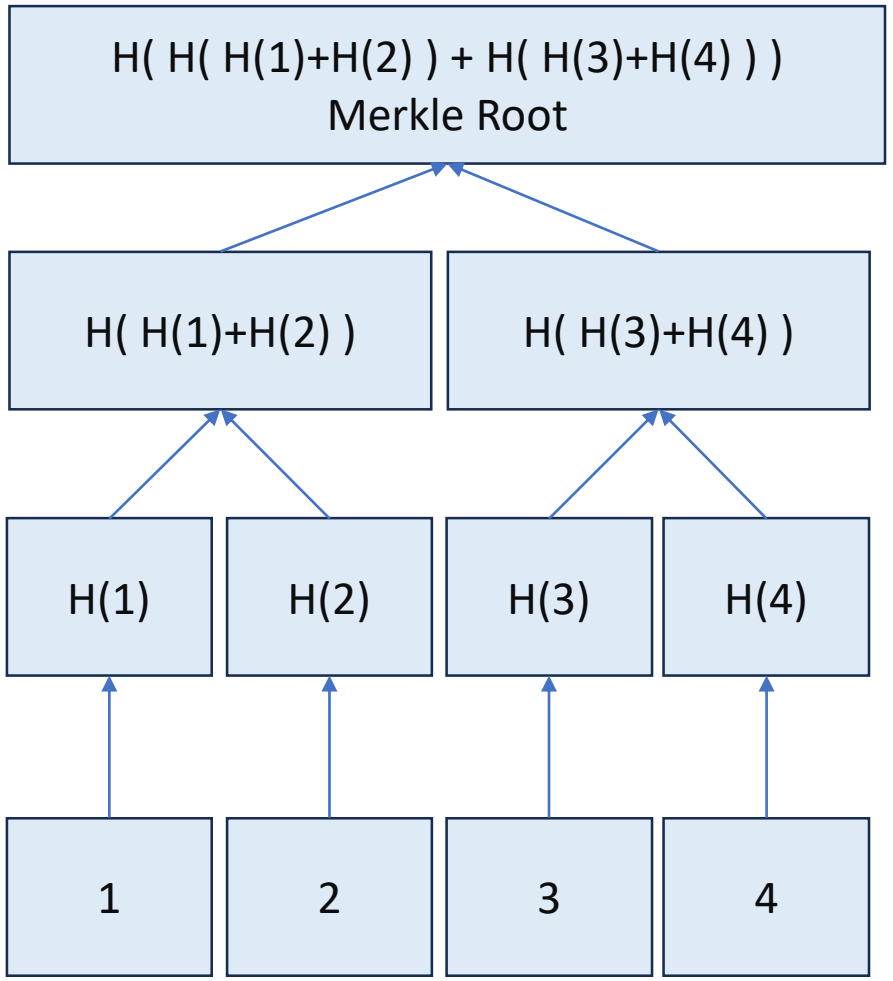
Facciamo una pausa dalla blockchain e vediamo cosa è «**Merkle Tree**»!

Trasferimento dati sul Internet



Ci sono 2 problematiche!

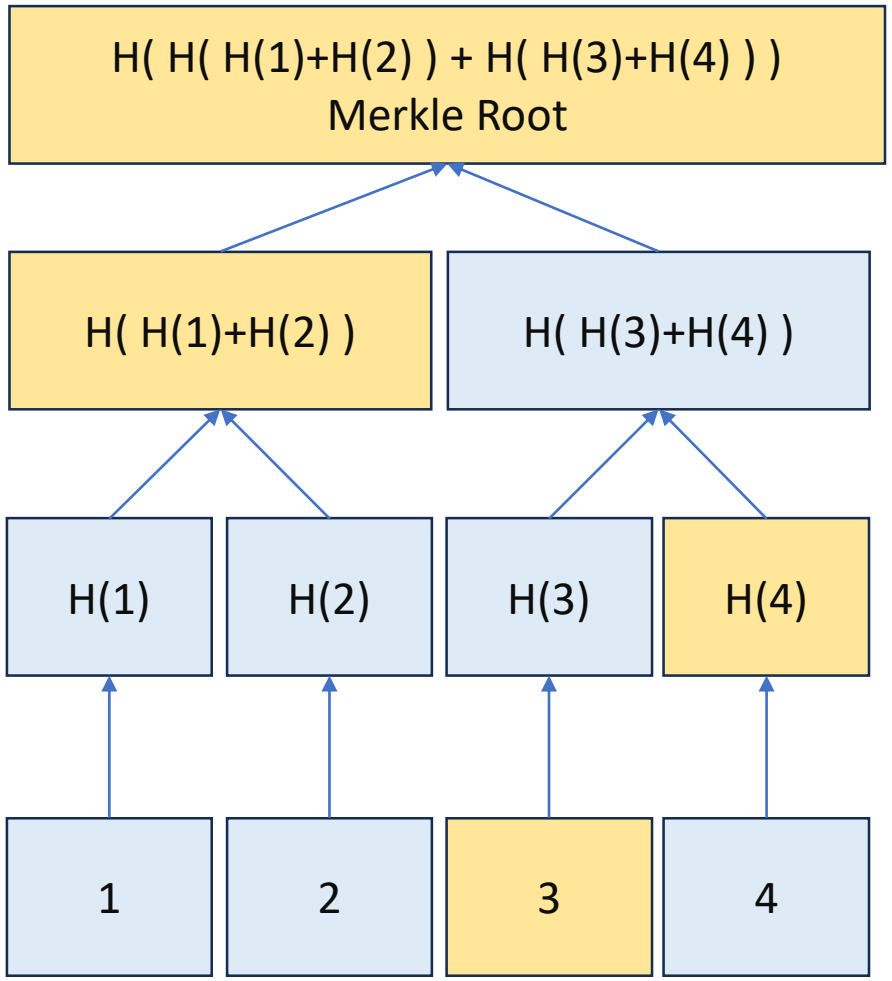
Merkle Tree protocollo viene utilizzato per trasferire qualsiasi cosa su Internet.



Always 32 byte length

SHA256 or faster hash algorithms

Merkle Tree Root Hash e Merkle proof sono necessari

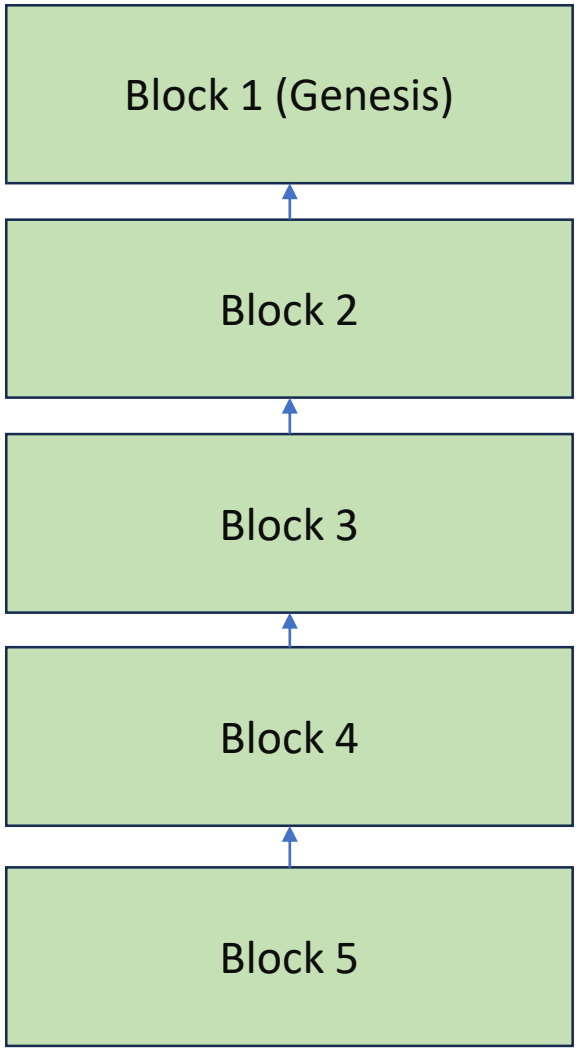


Data chunk number 3 + The proof

Ma cosa è Bitcoin?

Bitcoin è un sistema per implementare la scarsità digitale.

Distributed Ledger Technology **DLT**



Bob guadagna 50 monete.
Bob = 50

Bob da 10 monete ad Alice
Bob = 40
Alice = 10

Alice dà una moneta al bar e compra un caffe.
Bob = 40
Alice = 9
Bar = 1

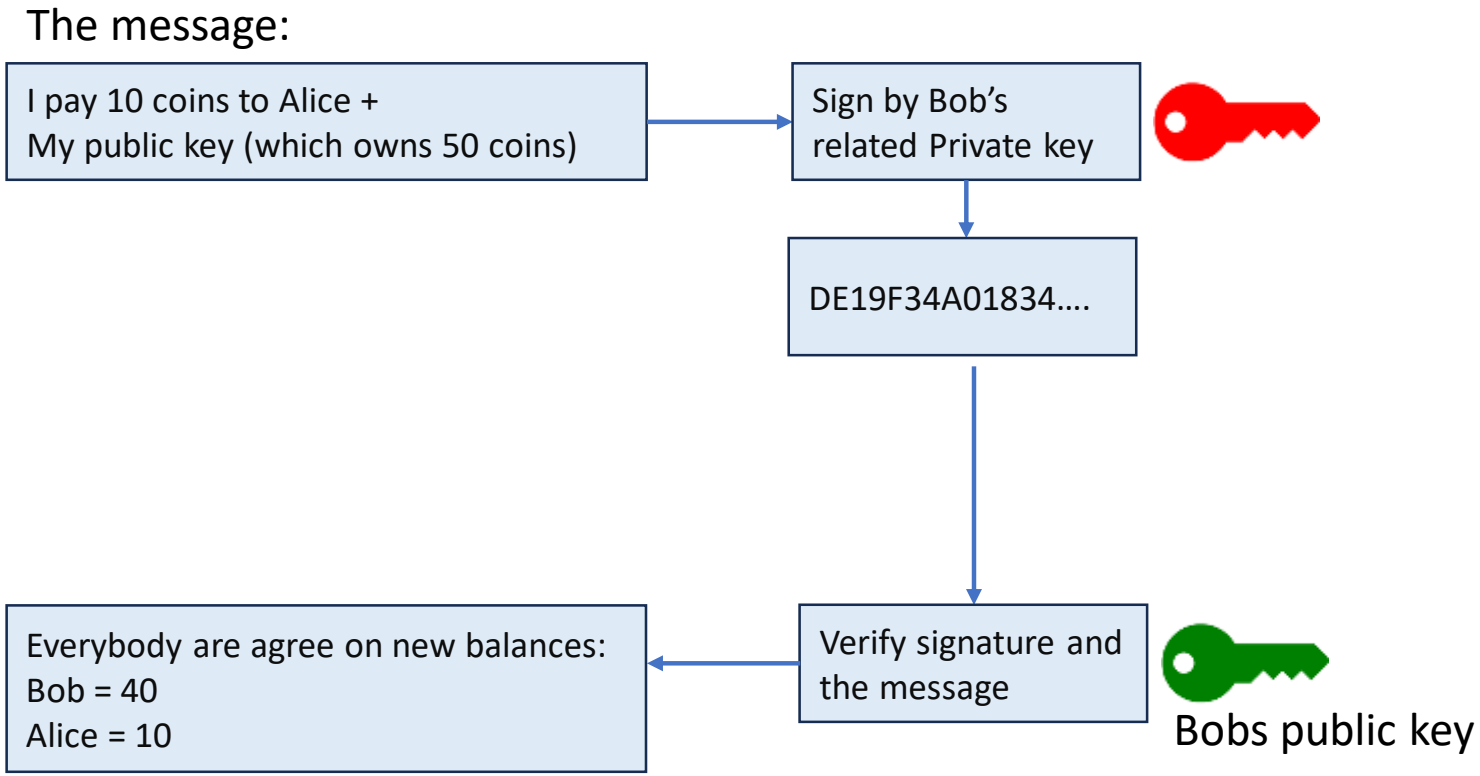
Tutti sanno tutto
Tutti controllano tutto
Tutti confermano tutto

Perche?
Perche,

Protocol is everything!

Asymmetric encryption

Come fa Bob a dimostrare di possedere le monete, e come fa a impedire che i suoi soldi vengano rubati?



Tutti sanno la chiave pubblico di Bob. Ma come fanno a saperlo?
Dalla transazione in cui ha ottenuto 50 monete!

Transaction explanation

Block 2

Bob guadagna 50 monete. => Il chiave pubblico «pub1» ha 50 moneti in possesso.

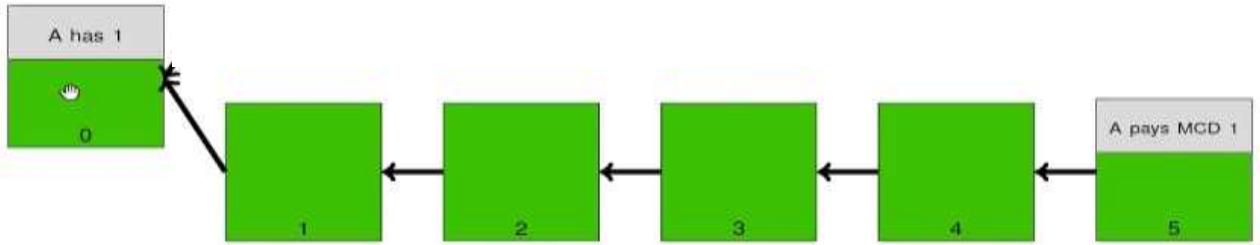
Block 3

Bob da 10 monete ad Alice (pub2 di Alice)
Bob = 40
Alice = 10

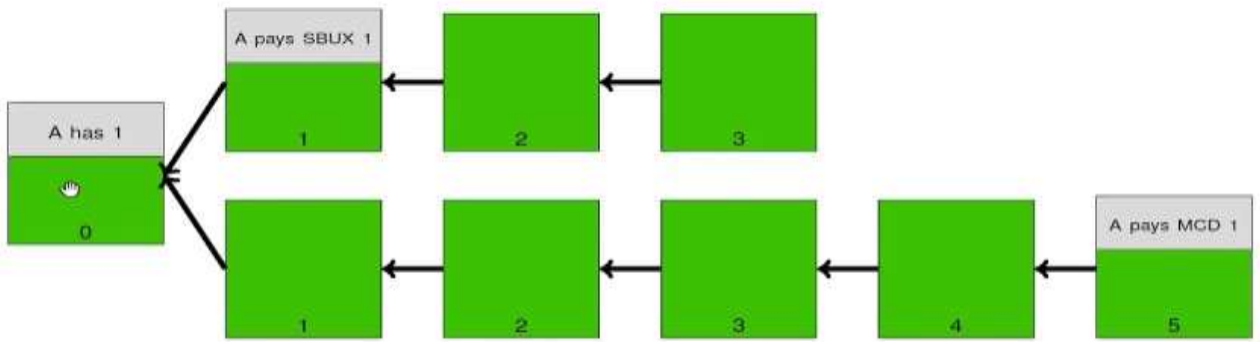
Bob si riferisce alla transazione nel secondo blocco.
E dice di vedere che io ho la chiave privata corrispondente all'indirizzo pub1.
E ora dico che trasferisci dieci monete dalla mia proprietà all'indirizzo pub2 (che in realtà è controllato da Alice).

Ma prima di tutto, come Bob ha guadagnato queste 50 monete?
Era regalo di vincitore! Chi che ha trovato il nonce giusto e creato il block nuovo.

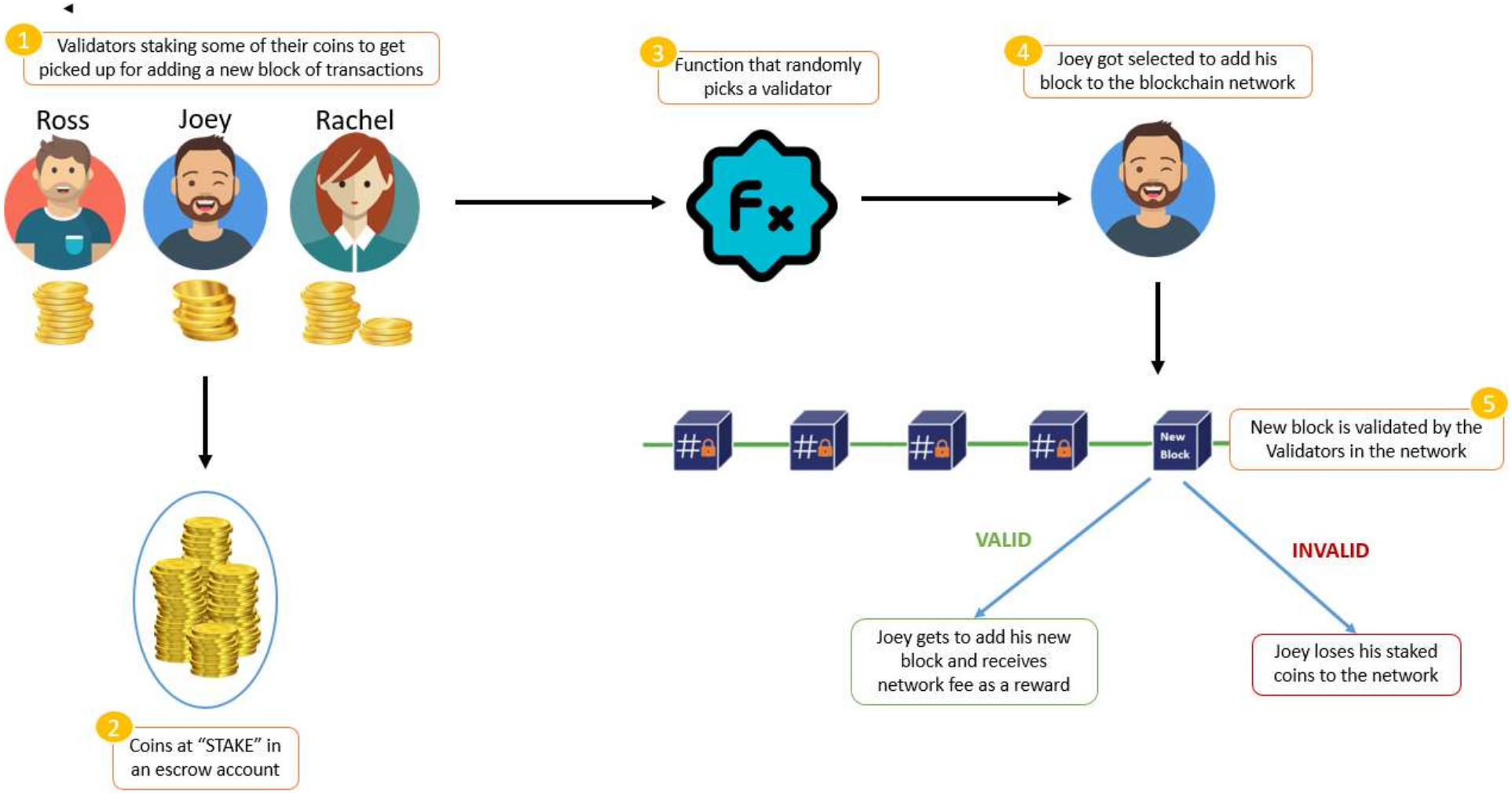
Double-spend attack



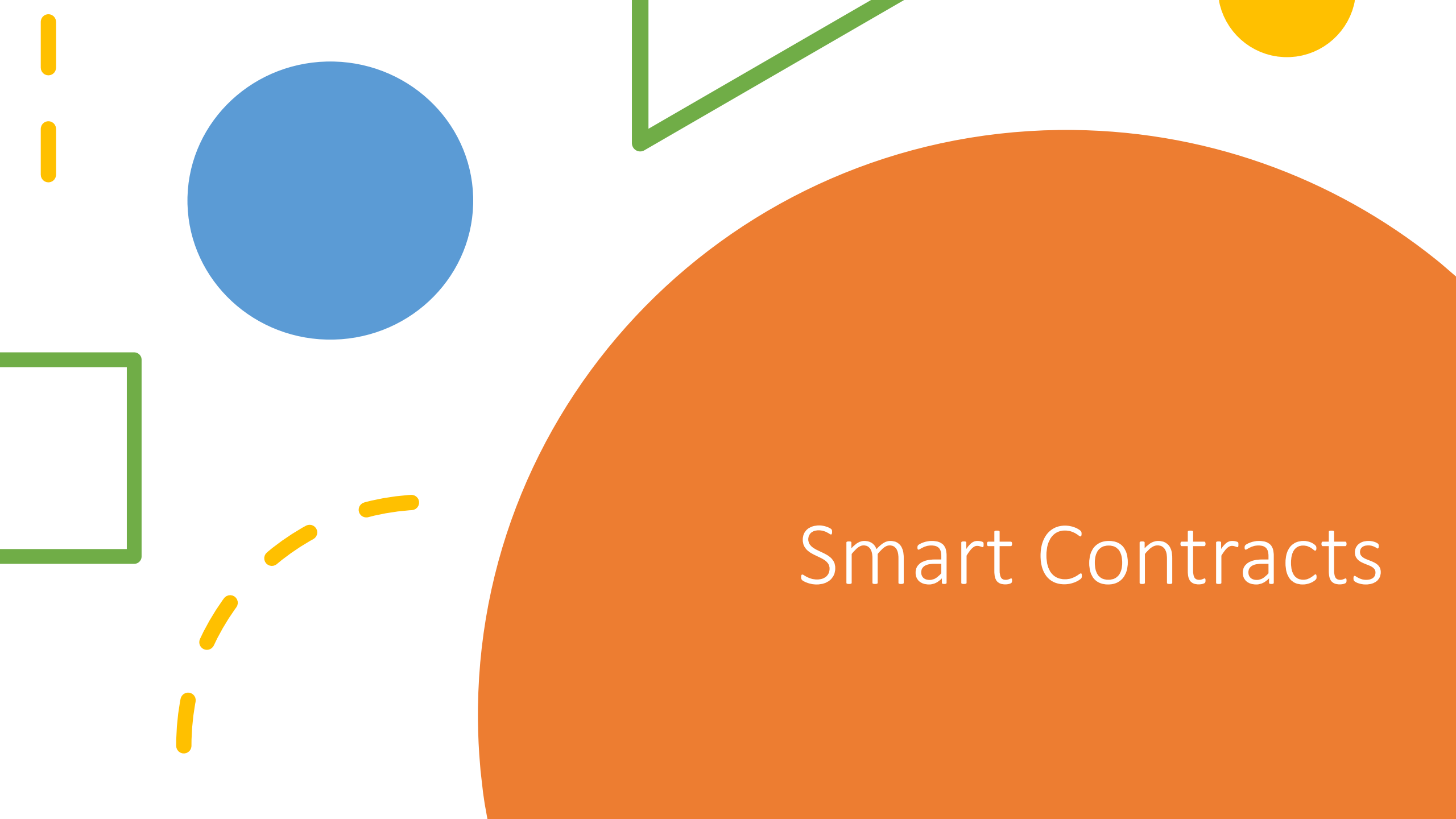
Solution Double-spend attack



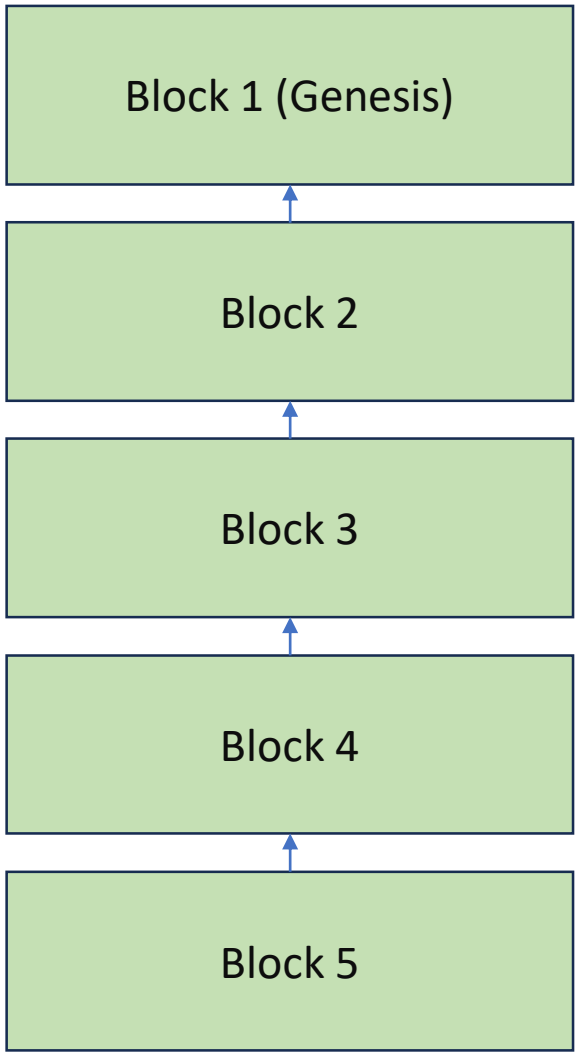
Proof of Stake



Proof of Work (PoW) VS Proof of Stake (PoS)


Smart Contracts

Distributed Ledger Technology **DLT**



Bob guadagna 50
monete.
Bob = 50

Bob da 10 monete ad Alice
Bob = 40
Alice = 10

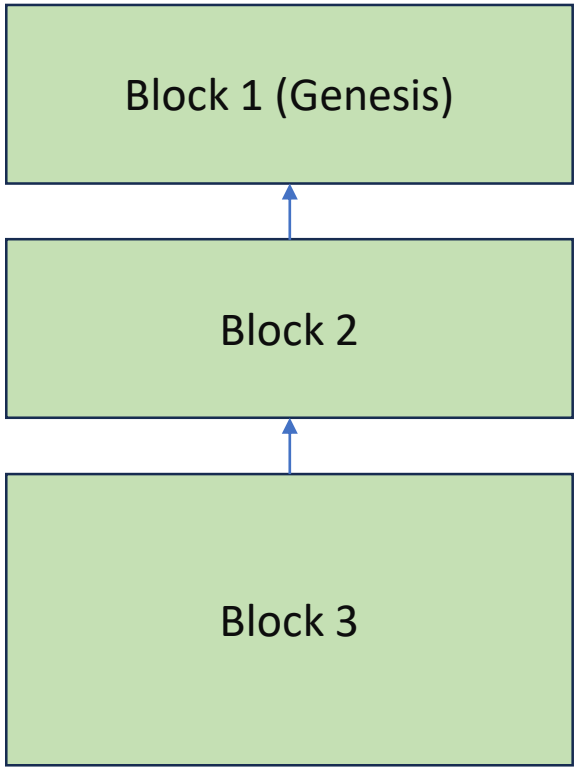
Alice dà una moneta al bar e compra un caffe.
Bob = 40
Alice = 9
Bar = 1

Tutti sanno tutto
Tutti controllano tutto
Tutti confermano tutto

Perche?
Perche,

Protocol is everything!

Distributed Ledger Technology **DLT**



Bob guadagna 50
monete.
Bob = 50

Bob pagerà 10 monete ad Alice, solo se
Già passato almeno 10 gironi da capodanno e Alice ha pulito casa di Marco e Toppo Gigio è d'accordo e firmato questo transazione e, … delle condizioni diversi (Turing complete machine)
Bob = 40
Alice = 10

Tutti sanno tutto
Tutti controllano tutto
Tutti eseguano tutti contratti (condizioni)
Tutti confermano tutto

Oracle (oracolo)

un servizio che fornisce dati al mondo reale a una blockchain

Alice ha pulito la casa di Marco?
Quanto è il tasso di cambio tra il Dollaro e l'Euro?
Quanto vale oggi l'azione di Apple?
Quale squadra ha vinto la partita tra Juventus e l'Inter?

Quanto arriverà il prezzo del petrolio?
Tesla aprirà una fabbrica a Berlino?
Chi sarà prossima presidente di stati uniti?

Utilizzi più comuni di Blockchain

- **Finanza**: La blockchain può essere utilizzata per creare sistemi di pagamento decentralizzati, come Bitcoin e Ethereum. Questi sistemi possono ridurre i costi e aumentare l'efficienza dei pagamenti internazionali.
- **Logistica**: La blockchain può essere utilizzata per tracciare i prodotti e le merci da un capo all'altro della catena di approvvigionamento. Ciò può migliorare l'efficienza e la trasparenza della catena di approvvigionamento.
- **Governo**: La blockchain può essere utilizzata per creare sistemi di voto elettronico e di registrazione dei voti. Ciò può aumentare la trasparenza e l'integrità delle elezioni.
- **Sanità**: La blockchain può essere utilizzata per creare registri sanitari decentralizzati. Ciò può migliorare la sicurezza e l'accesso ai dati sanitari.
- **Arte**: La blockchain può essere utilizzata per creare certificati di autenticità digitali per opere d'arte. Ciò può aiutare a prevenire la contraffazione.
- **Gestione della proprietà**: La blockchain può essere utilizzata per registrare la proprietà di beni, come immobili o opere d'arte. Ciò può rendere le transazioni immobiliari più efficienti e trasparenti.
- **Sicurezza**: La blockchain può essere utilizzata per creare sistemi di sicurezza decentralizzati. Ciò può migliorare la sicurezza delle reti e dei sistemi informatici.
- **Trasporto**: La blockchain può essere utilizzata per tracciare i veicoli e i loro carichi. Ciò può migliorare l'efficienza e la sicurezza del trasporto.