BLOCKCHAINLAB

Programmiamo la Blockchain

Strumenti e tecniche per programmare sulla blockchain

Francesco La Regina – Enzo Pastorelli
BLOCKCHAINLAB

Cosa è una criptovaluta?

È uno strumento per il trasferimento di valore

Crittografia a chiave pubblica/privata

UNA FAVOLA MEDIEVALE

- La Regina mette un messaggio nel suo scrigno
- Chiude tutto col suo lucchetto
  e manda ad Artù
- Artù aggiunge il suo lucchetto
  e manda indietro
- La Regina toglie il suo lucchetto
  e rimanda ad Artù
- Artù apre il suo lucchetto

Crittografia a chiave pubblica/privata

UNA FAVOLA MATEMATICA

Messaggio: 71
Coppia di chiavi di La Regina: 2 | 3
Coppia di chiavi di Artù: 5 | 7

- **La Regina calcola 71 x 2 x 3 = 426 e lo invia**
- **Artù calcola 426 x 7 = 2982 e lo manda indietro**
- **La Regina calcola 2982 / 3 = 994 e lo invia**
- **Artù risolve 994 / 7 = 142 / 2 = 71**

Funzioni HASH

- Output a lunghezza fissa
  per Bitcoin si usa SHA-256 con output di 2^{256} bit
- Facile da calcolare
- Resistente alle collisioni
- Irreversibile (a differenza della crittografia)
  se y = H(x) allora non esiste H^{-1} tale che $H^{-1}(y)=x$

ESEMPIO

H("Gatto") = "Go" H("Cane") = "Ce"

Perché le criptovalute sono rivoluzionarie?

Perché sono un asset digitale non duplicabile

Perché una criptovaluta non è duplicabile? Perché viene iscritta in un Ledger

Ledger e Blockchain

- Nel caso base il Ledger contiene un bilancio ossia una lista di coppie Indirizzo / Ammontare e le transazioni avvenute fra Indirizzi

- Il Ledger è archiviato in una Blockchain ossia una catena di blocchi di dati composti da:
  - un content (gli ultimi aggiornamenti al Ledger)
  - un header (i metadati e l'hash del blocco precedente a cui è indissolubilmente legato)

Perché il Ledger non è falsificabile?

Perché è condiviso sulla Blockchain e convalidato tramite Consensus

PoW (proof-of-work)

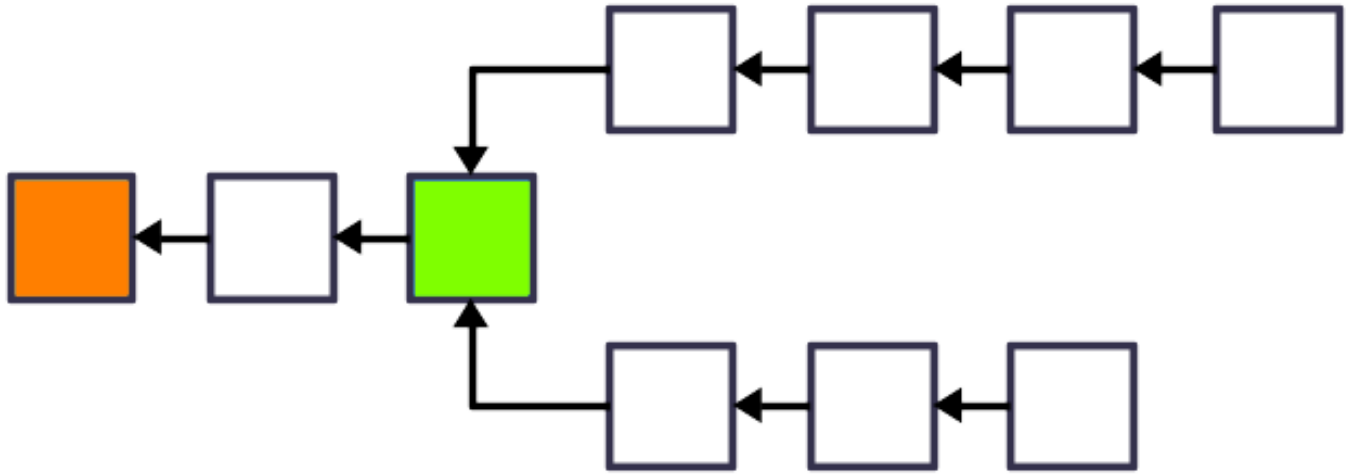
- Nel caso base la validità di un blocco è data da $H(B_x, H(B_{x-1}), rnd) > diff$

- Il calcolo viene effettuato dai Miner
  diff dipende dal numero di miner attivi
  0000000000007fb7db930261856af693cd7e2f1

- Il primo Miner che trova la soluzione distribuisce il nuovo blocco, tutti gli altri Nodi verificano

Fork, Soft Fork, Hard Fork

- Soft Fork: nuove regole più restrittive "retro-compatibile", non invalida i nuovi blocchi
- Hard Fork: nuove regole meno restrittive necessita consenso sulla validazione



Nuove regole

Vecchie regole


Quali evoluzioni?
→ Token
→ Smart Contract
Blockchain 2.0

Blockchain 2.0

- Lightning Network (secondo layer di Bitcoin, scalabile e programmabile)

- Hyperledger (permissioned, programmabile)

- Ethereum (pubblica, Turing equivalente)

- Unicalcoin (semi-privata, programmabile)


Grazie!
Domande?

BLOCKCHAINLAB