
proofOfState
Links
Nonce
blockchain
verifiers
rewarded
Avalanche
linked
transaction
fingerprint
miners
majority
transactions
chain
block
distributed
records
permissioned
nodes
ledger
attack
permissionless
cryptocurrency
verify
cryptographic
Bitcoin
proofOfWork
hash
mining

A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

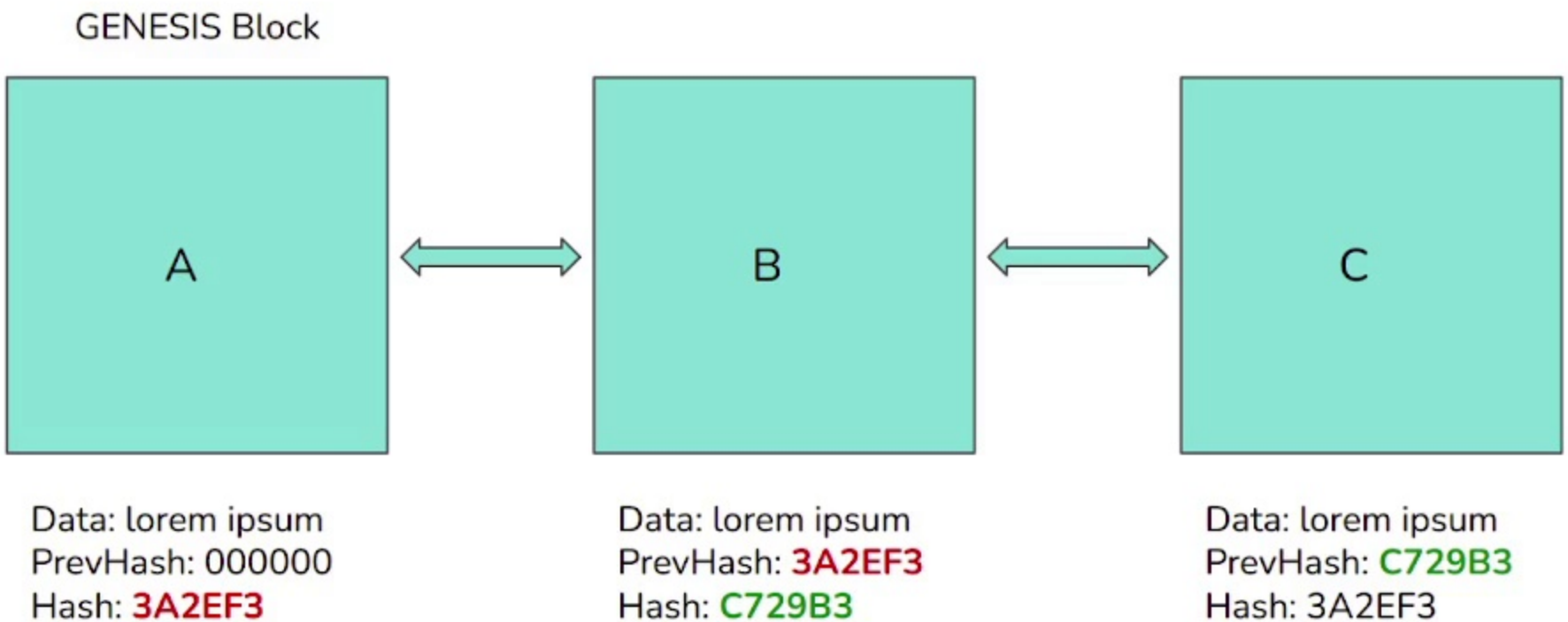
– *Wikipedia*

Where the Idea come from?

- In 1991, Stuart Haber & W. Scott Stornetta published a paper “How to Time Stamp a Digital Document”.
- Later,the blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin.

What is BlockChain?

- Chain of blocks which contains some data.



Block

Fields in a typical block:

- Block No
- Nonce
- Transactions
- Previous Block's Hash
- Current Block's Hash

Courtesy: https://www.superdatascience.com/pages/blockchain

Cryptographic Links

- Links should be :
  - One Way
  - Avalanche Effect
  - Deterministic
  - Fast Verification
  - Negligible Collision Probability

SHA-256
e3b0c44298fc1c149afbf4c899
6fb92427ae41e4649b934ca4
95991b7852b855

Courtesy: https://pngimg.com/image/67847

Ledger

- A ledger is a book or collection of accounts in which account transactions are recorded.
- Can easily be manipulated and compromised.

Courtesy: https://en.wikipedia.org/wiki/File:Ledger.png

Immutable Ledger

- Blockchain can also be considered as Immutable Ledger where each block represent the page in the ledger.
- Immutable because it is practically impossible to alter any block due to cryptographic links.
- Important protocols:
  - Longest Chain wins
  - 51% rule