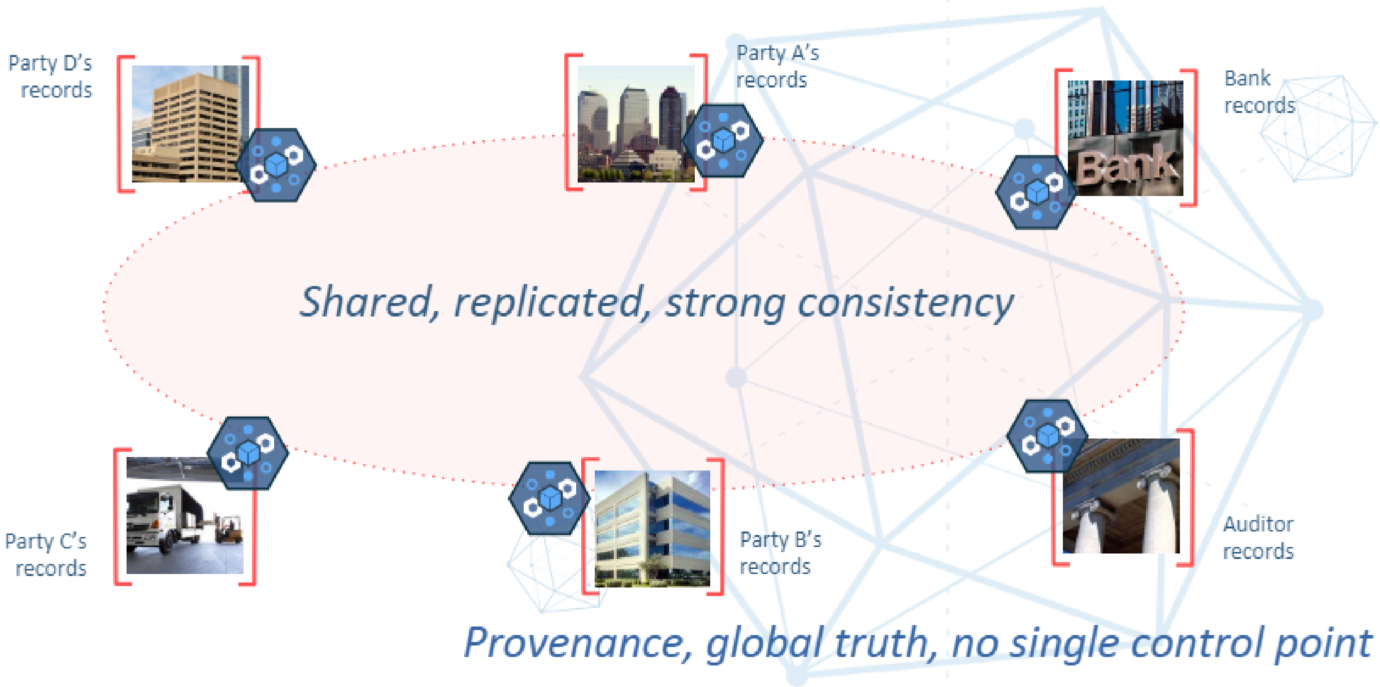
Blockchain: A shared distributed ledger allowing participants in a business network to work with one system of record



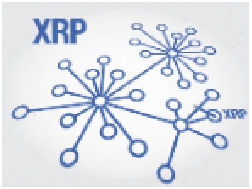
Shared, replicated, strong consistency

Provenance, global truth, no single control point

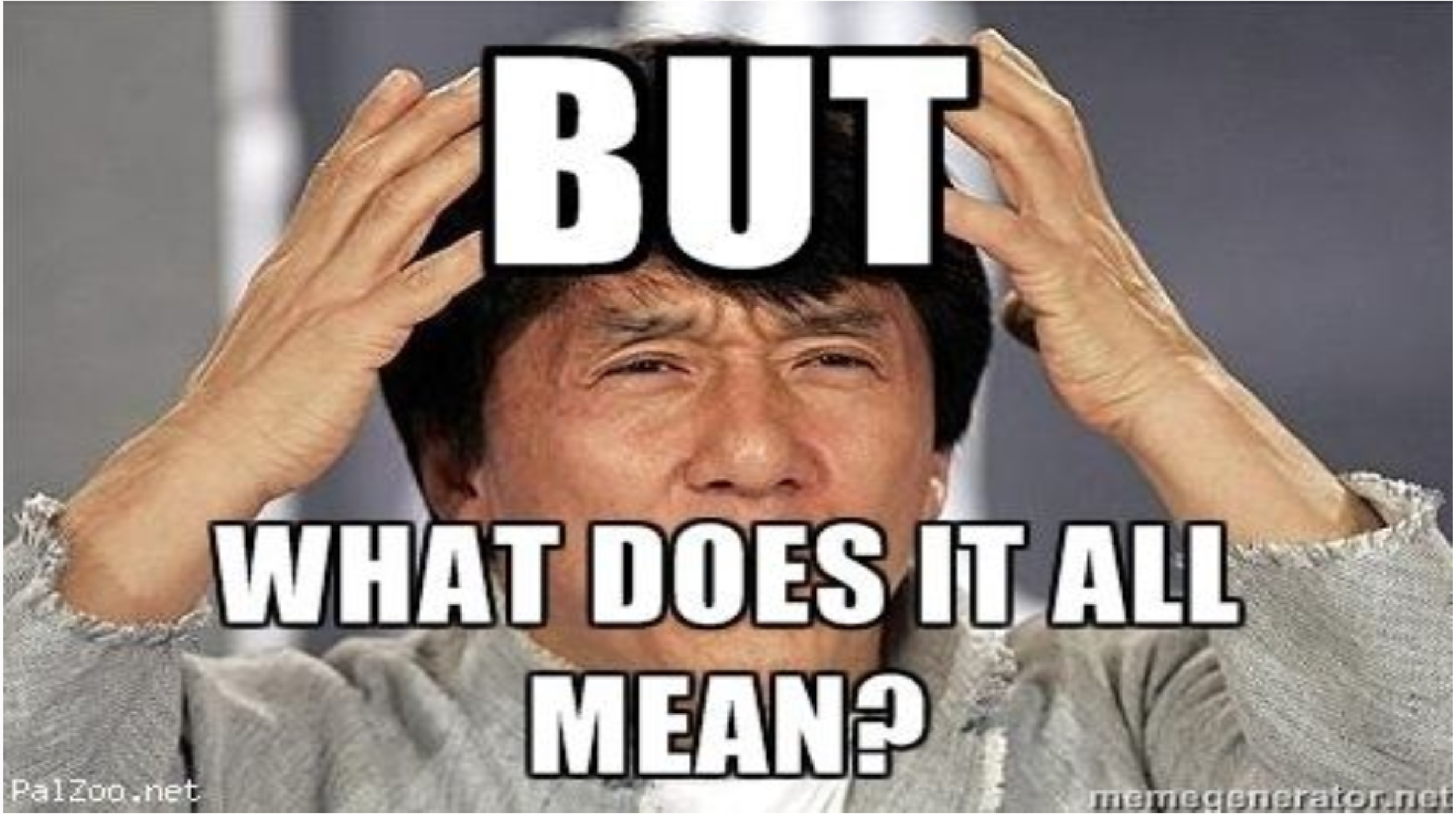
Blockchain

- Introduced in 2008 [Bitcoin08]
- **Decentralized** networks to decide on the order in which network **transactions** are **validated** & append to a system wide ledger
  - **Decentralized**: network controlled by independent entities
  - **Transactions**: messages announced across the network
  - **Validity**: following specified set of rules

ETHEREUM



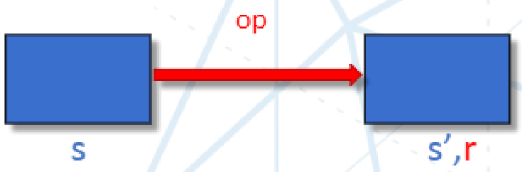
ripple



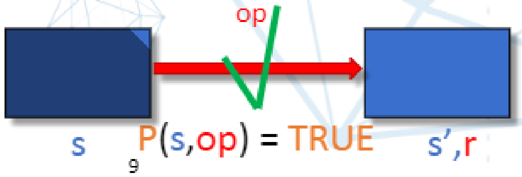
A state machine

- Define a functionality F
  - ✓ Operation op transforms a state s to new state s’ and generates response r

$$F(s,op) \longrightarrow (s',r)$$

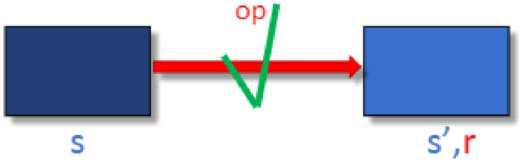


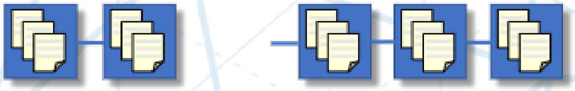
- Validation
  - ✓ Operation has to be valid according to a predicate P



Blockchain state machine

- Append-only log
  - ✓ Every operation op appends a ”block” of valid transactions to the log

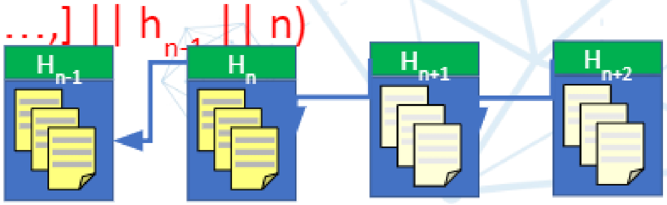




- Log content is verifiable from the most recent element

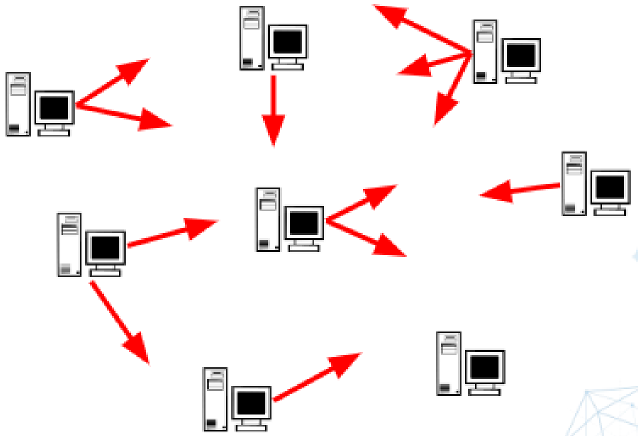
- Log entries form a hash chain:

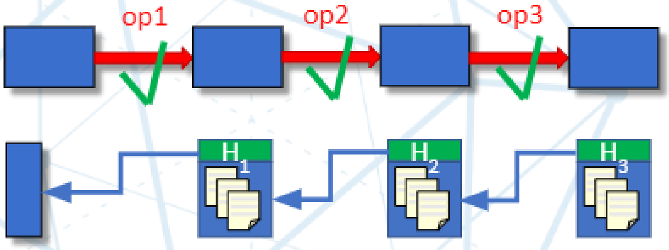
  $h_n \leftarrow \text{Hash}([tx_1, tx_2, \ldots,] \,||\, h_{n-1} \,||\, n)$



Distributed peer-to-peer protocol to create a ledger

Nodes produce new transaction





Nodes run a protocol to construct the ledger

Blockchain protocol features

- Only ”valid” operations (transactions) are “executed”

- Primitive transactions such as in Bitcoin
  - ✓ Statement of ownership for crypto coins:
    “X amount of bitcoins belongs to Y” signed by Z

- More complex transactions (AKA smart contracts == arbitrary code)
  - ✓ Encapsulate business logic that responds to events (on blockchain) and may produce response by for example transferring asset
  - ✓ Auction, elections, trading, investment decision, supply chains, etc…

Blockchain security

- Transactional privacy
  - ✓ Anonymity or pseudonymity through cryptographic tools

- Smart contracts privacy
  - ✓ Distributed secure computations on encrypted data
    - ZKP, Homomorphic encryption

- Accountability & non-repudaiation

- Auditability & transperancy
  - ✓ Hash chain

Conflict
Resolution