PoIS Concepts

Team 22: se7en

Refreshing the PoIS Concepts Required for Video

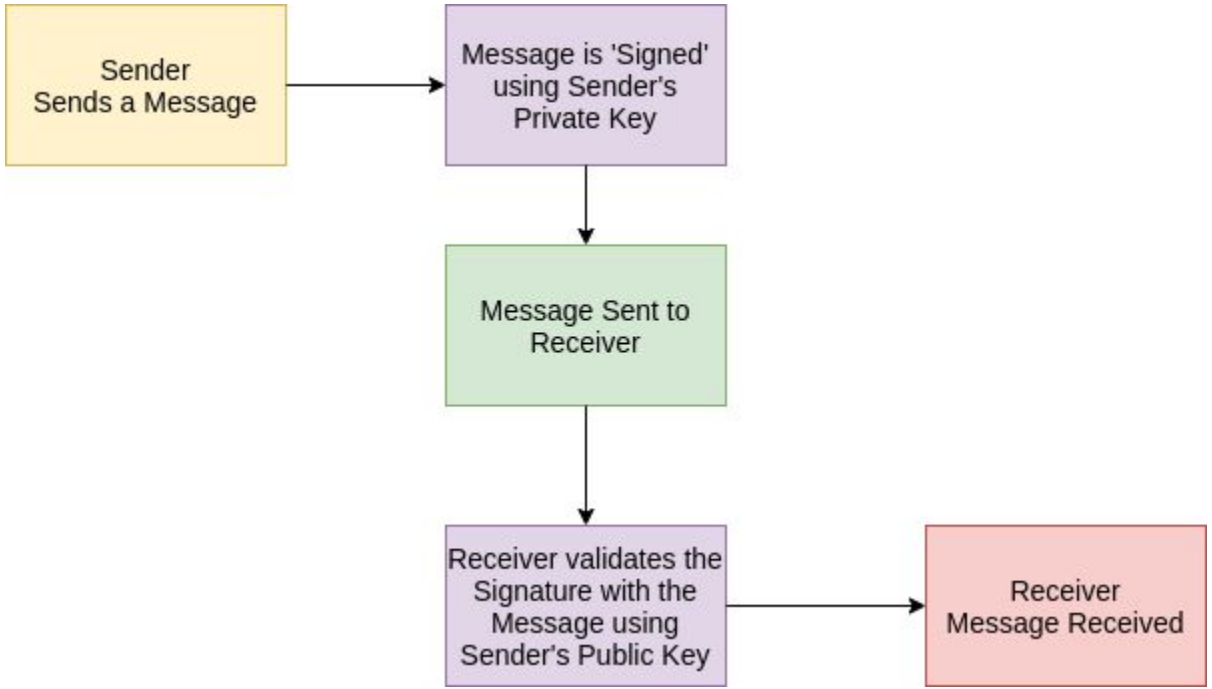
Digital Signatures

- A Mathematical Scheme used to verify authenticity of Digital Documents
- Uses Public Key Encryption
- Provides Non-Repudiation by the signer
    - Signer can’t refuse he/she didn’t sign the document. All this is done while keeping the Private Key secret

Digital Signatures

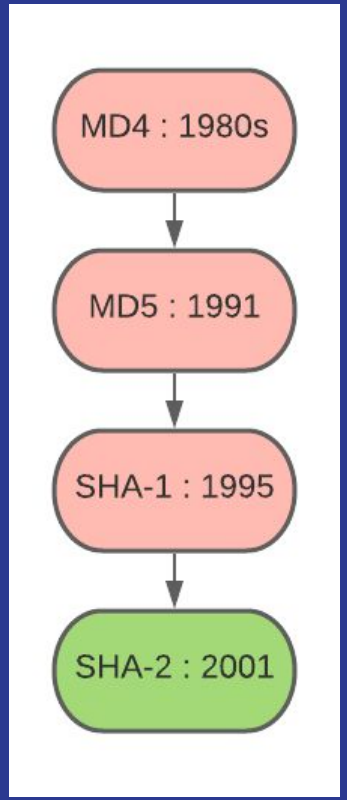
- Mathematically consists of three parts
  - Generating Public and Private Key
  - Generating a Signature using a Private Key and String
  - Validation of Signature using a Public Key and Message
- Elliptic Curve Digital Signature Algorithm - State of the Art.
  - Used in BidKarona

Successful Transfer using Digital Signatures

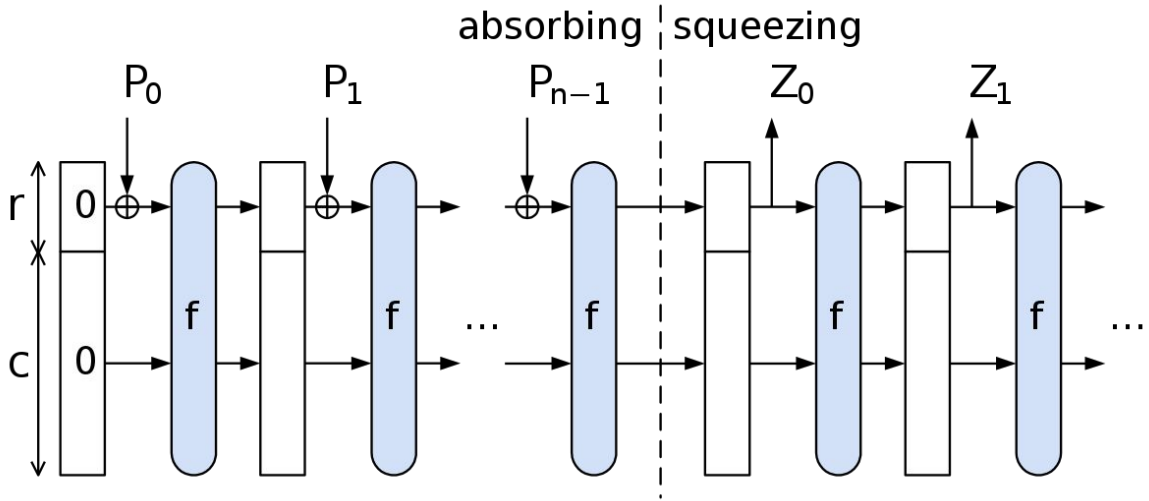


Keccak-256

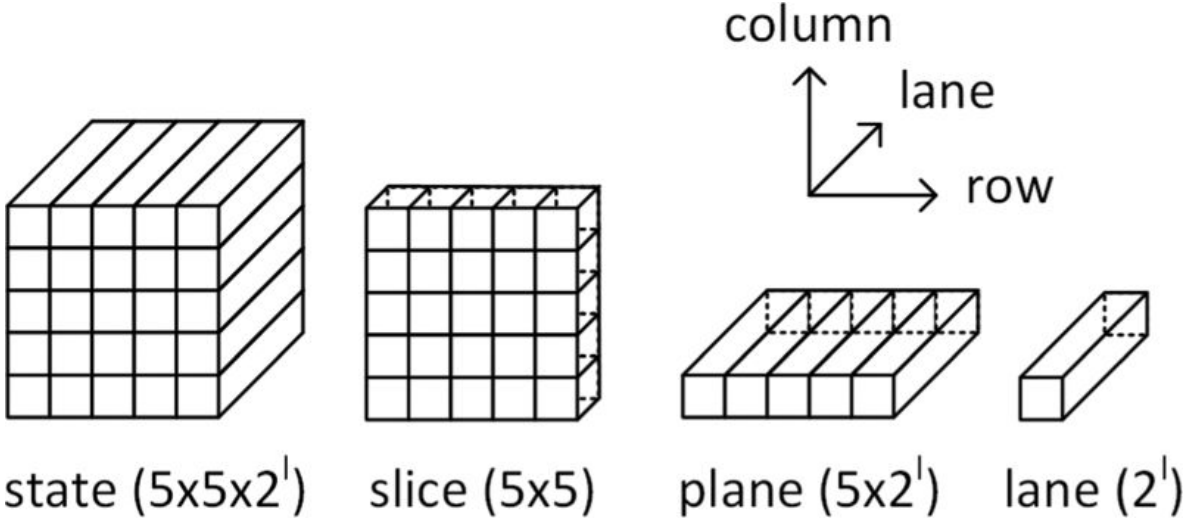
2012



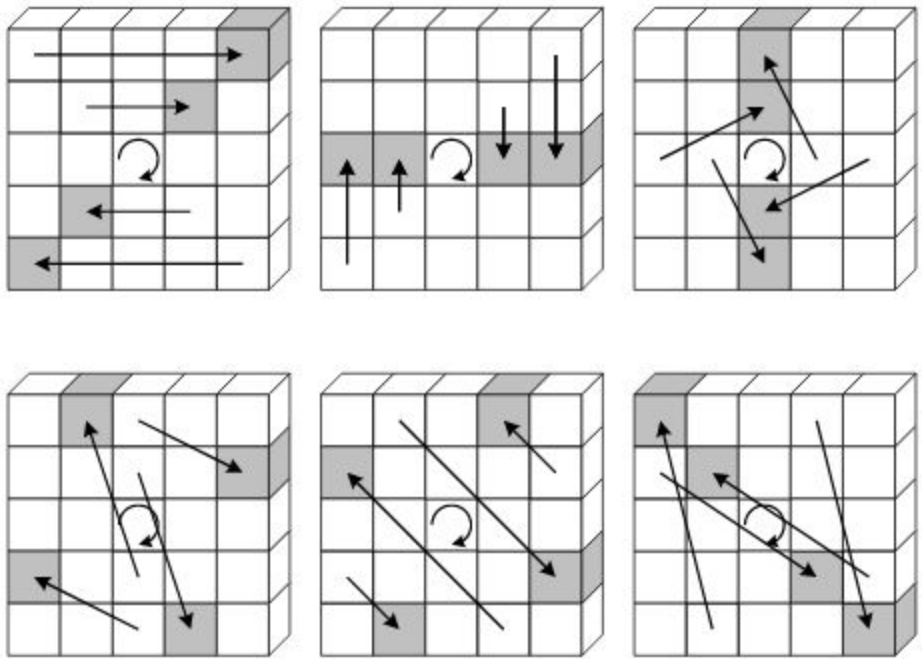
Sponge Function



State Transformation



Permutation Operation



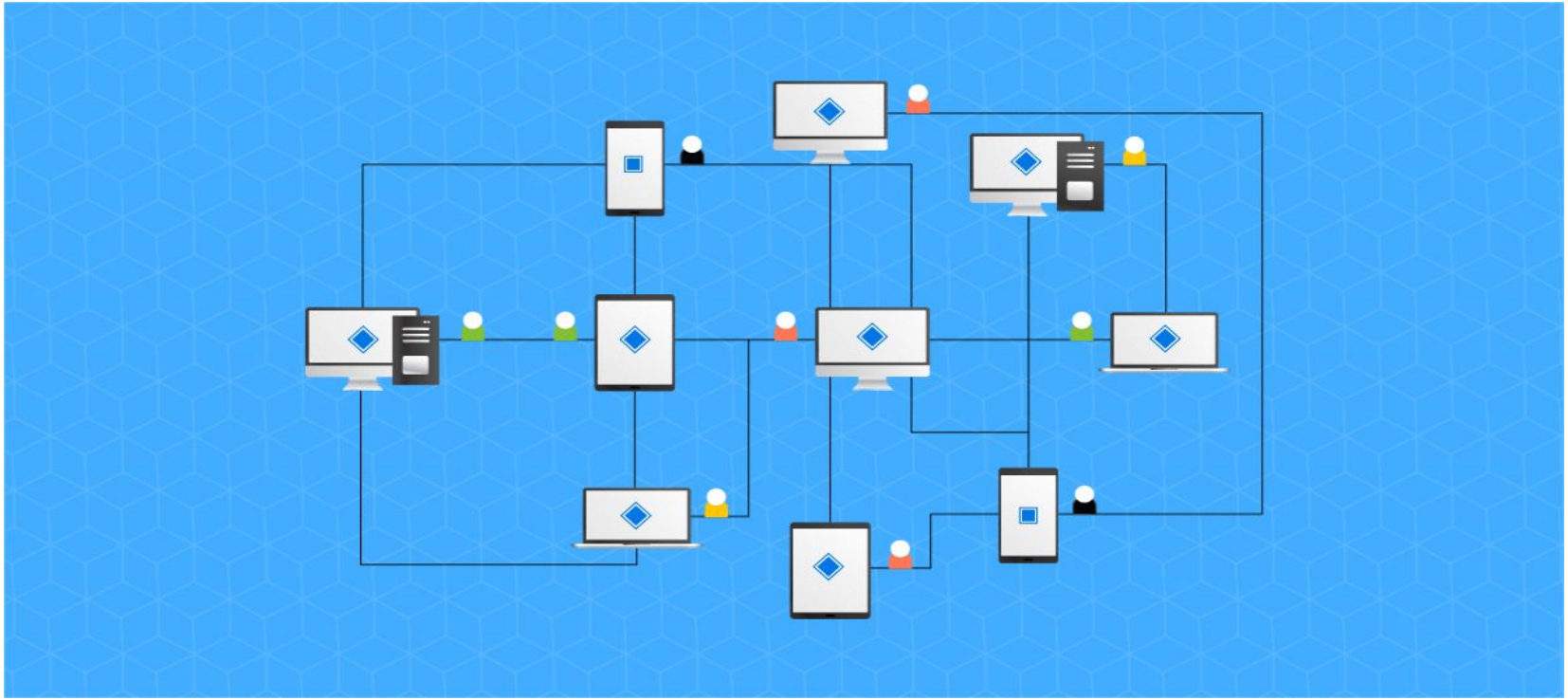
- **A′[x, y, z] = A[(x + 3y) mod 5, x, z]**

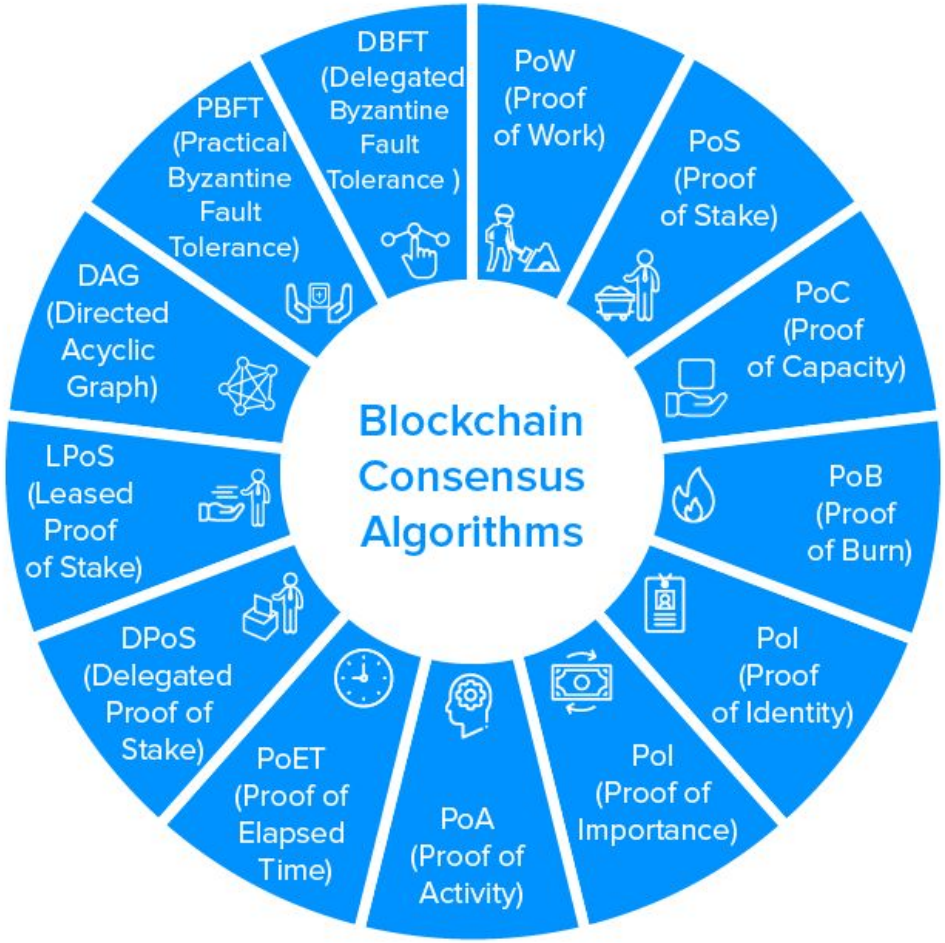
Multiple Rounds of 5 operations

$$\mathrm{Rnd}(\mathbf{A}, i_r) = \iota(\chi(\pi(\rho(\theta(\mathbf{A})))), i_r).$$

Proof of Work for Consensus

Why Consensus mechanism?




Blockchain Consensus Algorithms
PoW (Proof of Work)
PoS (Proof of Stake)
PoC (Proof of Capacity)
PoB (Proof of Burn)
PoI (Proof of Identity)
PoI (Proof of Importance)
PoA (Proof of Activity)
PoET (Proof of Elapsed Time)
DPoS (Delegated Proof of Stake)
LPoS (Leased Proof of Stake)
DAG (Directed Acyclic Graph)
PBFT (Practical Byzantine Fault Tolerance)
DBFT (Delegated Byzantine Fault Tolerance)

Proof of Work

- Consensus mechanism used by Ethereum
- Miners solve complex mathematical *puzzles*
- Solving these puzzles requires extensive computing power
- Nonce

The infamous *51% Attack*

- A group of users control the majority of mining power
- Attackers monopolize the creation of new blocks and earn all the rewards