Blockchain Addresses

Objective: To Understand concept of Mining in Bitcoin Network.

Blockchain = Distributed Ledger

- Distributed
  - Everynode has digital copy of blockchain database.
  - All nodes can contribute in it.
- Maintained by Consensus
  - Consensus is governance mechanism that gurantees that records / database is tampre proof.
  - Transactions can be done only with **agreement** of all relevant parties.
- Immutable
- Auditable

Blockchain = Distributed Ledger

- Immutable
  - Once consensus is reached on validity of transaction / data and recorded on blockchain then it cannot be **changed or deleted.**
- Auditable

Blockchain = Distributed Ledger

- Distributed
  - Everynode has digital copy of blockchain database.
  - All nodes can contribute in it.
- Maintained by Consensus
- Immutable
- Auditable

Blockchain = Distributed Ledger

- Distributed
  - Everynode has digital copy of blockchain database.
  - All nodes can contribute in it.
- Maintained by Consensus
- Immutable
- Auditable

Types of Blockchain

- Public Blockchain
- Private Blockchain
- Consortium Blockchain
- Hybrid Blockchain

Public Blockchain

- Open to all
- Anyone can join and become Full / Partial Node.
- Can read whole state of chain.
- Its permissionless type of blockchain
- Bitcoin, Litecoin are example of public blockchain

Consensus Mechanism

- Are the methods to solve the problems.
- There are several methods to achieve the consensus.
  - eg. delphi, Nominal Grouping
- Consensus in blockchain ensures that all nodes are agree on one sloution / order and record can be added as its immutable.

Why Consensus Protocol

- Unified Agreement
- Fault Tolerant
- Collaborative & Participatory
- Egalitarian
- Incentivistaion
- Prevent Double Spending

Consensus Mechanism

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Proof of Authority (PoA)
- Proof of Elapsed Time (PoET)

PoW

- PoW is most well known consensus used in Blockchain.
- Several nodes compete to find solution to complex mathematical problem based on cryptographic hash.
- Solution found is called PoW.
- Miniers release their PoW to others for verification to reach consensus.
- This Solution is difficult to produce but easey to verify.
- Whole process is extensively computation intensive.
- First Miner get rewarded to produce PoW.

PoW

- Disadvantages:
  - Time – Consuming
  - High Energy Consumption
  - 51% Risk

- eg. bitcoin, litecoin, Dash, Monero and Etherium

PoET

- Proof of Elapsed Time
  - Concived in 2016.
  - Commonly used in Permissioned Blockchain.
  - Based on fair lottery system where each node is equally likely to be a winner.
  - Each Minor node in blockchain network provided with random timer object from trusted code.
  - Method aims to prevent any attempt by minner to get a shorter period.
  - Mechanism similar to PoW.
  - Also in PoET identity of Miner is kknown unlike PoW.

PoET

- Disadvantages:
  - Vulnerability
  - Relies heavily on use of Trusted Execution Enviroment (TEE).
  - Intel SGX-Enabled CPU
  - Vulnerable to other security attack like Foreshadow which attack on Intel-SGX.

- eg. Hyperledger Sawtooth uses PoET

PoS

- Implemented in 2012 for Peercoin.
- The more stake one has in validating node, less chance one will be tempted to corrupt the validating process.
- Users with higher stakes will have most interest in maintaining and securing n/w.
- To keep n/w reputed and avoid diminishing it.
- Mining nodes are called as validators / Forgers / delegates.
- Forger has to commit his / her stake in the network as collateral to be in the running for chance to validate the transaction.

PoS

- Algorithm will randomly select forger based on stake he put forward.
- Validating nodes can forge or create blocks proportional to the amount they have staked.
  - eg. 10 % stake can validate 10% Txns.
- Disadvantages
  - Cheaper to attack
  - Centralization Risk
- Eg Peercoin, NXT, Blackcoin, Etherium uses PoS over PoW

PoS

- Delegated PoS

PoA

- Proposed in 2017
- Similar to PoS and DpoS
- Only group of preselected authorities called validators secure blockchain and can produce new block.
- Instead of staking coins or currency here identity is staked.
- Identities are public and verfiable by third party

PoA

- PBFT
- RAFT