# Blockchain Platforms and Consensus

Wednesday, December 21, 2022 2:56 PM

Types of blockchain platforms -

Permissionless blockchain -

- Also known as public blockchain
- They allows anyone to access the network
- Anyone with computer and internet can join the network
- Data is accessible to everyone
- Anyone can validate or take part in a transaction
- Highly transparent
- Completely open source
- High level of decentralization
- Slow as large number of users are involved in the network
- Low energy efficient

Permissioned blockchain -

- Also known as private blockchain
- They only allows limited users to access the network
- Permission is required to access the data inside the network
- Only few selected users take part in transaction validation
- Low decentralization as compared to permissionless blockchain
- Fast as network is small
- Not that much transparent
- Not trustable as control is in the hands of few group of people
- Offer customization

Public blockchain -

- It is open to everyone having computer and internet
- It is the most decentralized network
- No restrictions inside the network
- Used where high transparency is required
- Trustable
- Slow as Proof of work or Proof of Stake is required to verify the transaction
- Energy consumption is high
- Ex. Bitcoin, Ethereum

Private blockchain -

- It is restricted to a group of people or an organization
- It is used for personal purpose by an organization
- Only few people can access the data
- Permission is required to access the data
- Less transparent
- High processing speed
- Non trustable

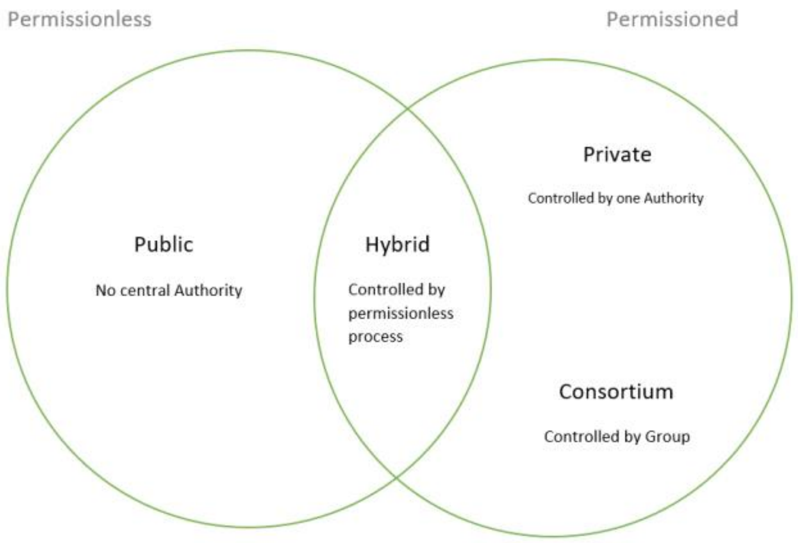
- Ex. Hyperledger, Corda

Hybrid blockchain -

- It is the combination of both public and private
- It is very flexible in nature
- According requirements it can implement features of both public and private blockchain
- Cost is very low as compared to others
- Ex. Ripple network

Consortium blockchain -

- When more than one organizations want to form a blockchain network for certain purpose it is known as Consortium blockchain
- It is federal blockchain where one or more organization joins the network
- It also comes in permissioned category
- Decision making is diffcult
- Used to solve organization's problem
- Some part is private and some is public
- Problem of vulnerability
- Ex. Tendermint and Multichain



Ethereum -

- Ethereum is a blockchain platform having its own cryptocurrency as Ether or ETH
- It is widely used in digital transactions, NFT, DeFi and in other fields
- ETH is second popular cryptocurrency after Bitcoin
- Ethereum provides platform to run many Smart contracts
- Also it provides access to dApps using smart contracts
- Recently Ethereum shifted from Proof of work to Proof of Stake

Hyperledger -

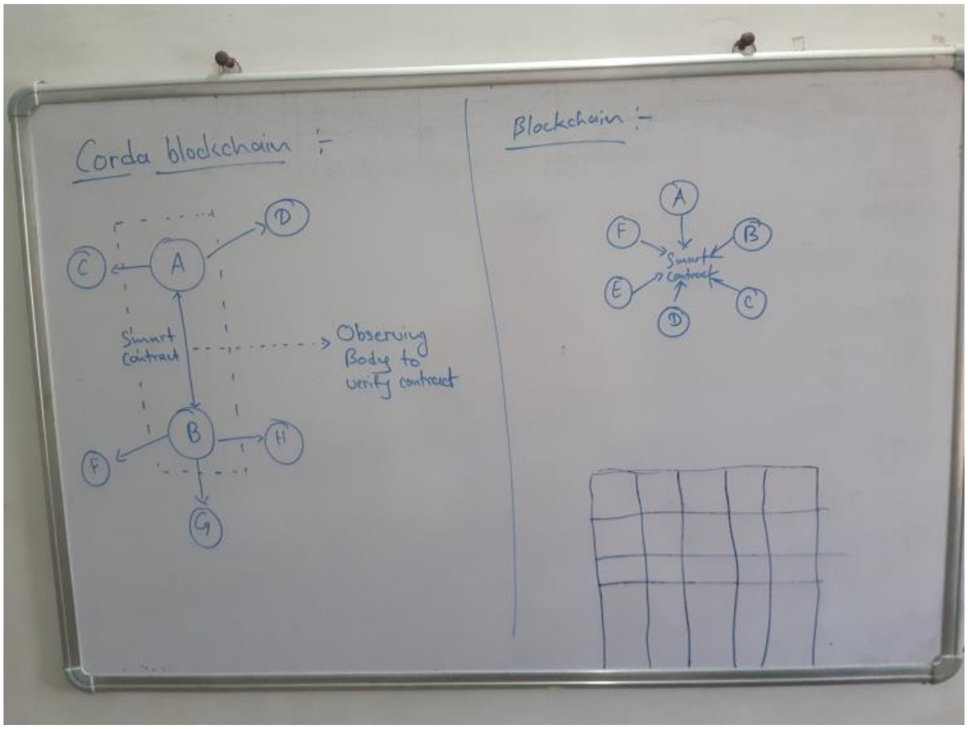
- Hyperledger is an open source project hosted by Linux foundation
- It is collaborative project in which many global enterprises are contributing
- It is not a blockchain, not a crypto currency
- Bitcoin and Ethereum are public blockchains and are used in point of view of B2C (Buisness to Customer)
- For B2B these can not be used so for that Hyperledger project is working on
- It focuses on many areas like banking, industry, health, manufacturing, etc.
- It comes under permissioned blockchain
- There are many frameworks for its development like Fabric and Indy
- There are also many tools for its development like Composer, Explorer, etc
- Fabric has concept of subnet in it to maintain privacy between two nodes in the same network
- We can do development in Fabric using Chaincode
- We can use JS, JAVA and Golang to code in Chaincode
- The ledger in fabric has two components
- One is to store state of asset
- Second is to store transaction history of asset

IoTA -

- It is a distributed ledger used to conduct transactions between devices in a IOT ecosystem
- Its cryptocurrency is MIOTA
- IOTA uses a method called TANGLE for verifying transactions
- It comes under permissionless blockchain
- MIOTA is premined means before launching MIOTA the coins or tokens of MIOTA are mined
- These saves mining cost and energy
- IOTA uses Tangle for efficient memory management
- Tangle is a Decentralized Acyclic Graph (DAG) which is a system of nodes which are not sequential
- Nodes are simply devices connected to the network
- In Tangle transactions can be processed simultaneously.
- In Bitcoin the systems having full nodes have to verify a transactions by processing it
- In Tangle a transaction is verified by referencing to two previous transaction and this saves energy and time
- Also it uses POW as last step to verify transaction
- IOTA's has many technical flaws
- It is vulnerable to cyber attacks
- It does not uses SHA256 for encryption and uses its own encryption which is flawed
- It uses a central authority to verify transaction and this is not true decentralization

Corda -

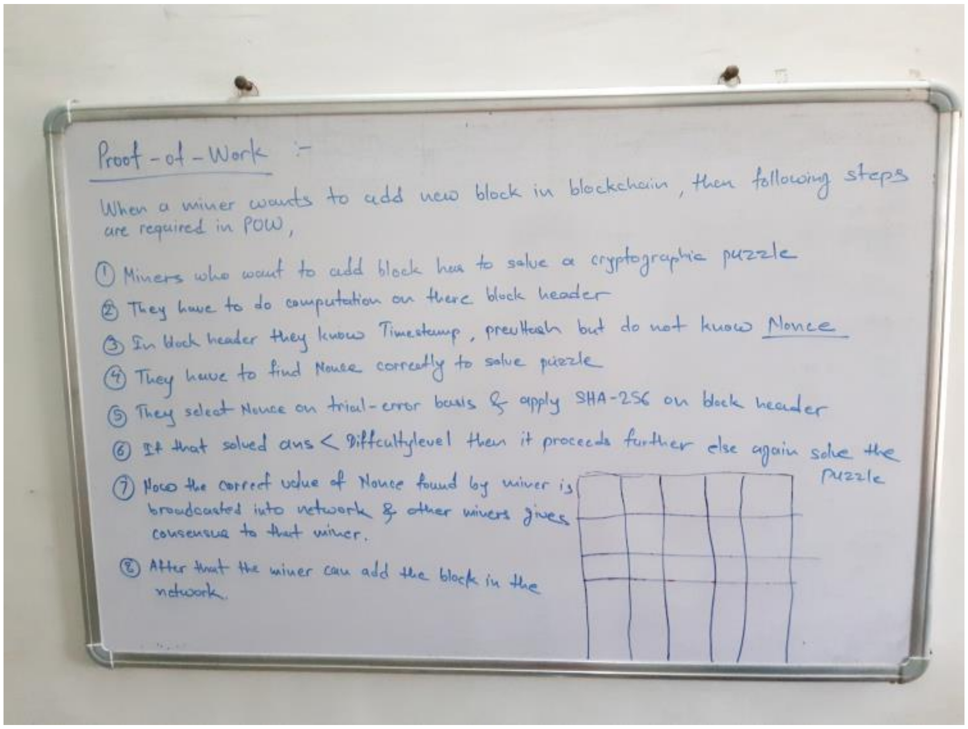
- Corda is a distributed ledger platform
- It is a permissioned blockchain technology or private blockchain
- It is developed by an organization called as R3
- It is mostly used in enterprise market by big enterprises to perform smart contract
- It is uses different method to validate or perform a smart contract
- The data of smart contract is only visible to those nodes who are involved in it
- The smart contract is verified by an observing body or regulatory body to maintain security
- In corda the blocks are not connected instead the transactions are connected with their hash values



Consensus in blockchain -

- Consensus is a decision that is taken by multiple nodes in a blockchain to verify a transaction
- In public blockchain anyone can add new blocks in network by mining
- Now which block is to add in network is decided by consensus
- The block is broadcasted in the network
- If more than 50% of nodes give there consensus then that block can be added into the network
- A consensus mechanism is a set of rules or methods to verify or accept a new block in network
- A consensus is a method to achieve trust, agreement across the decentralized network

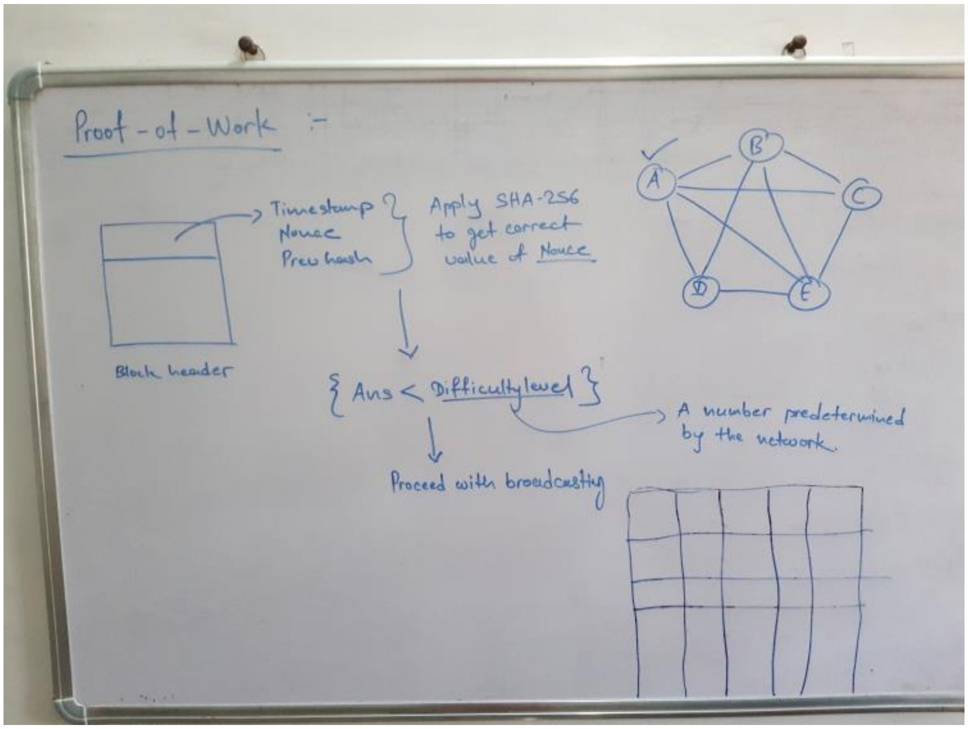
PoW (Proof of Work)-



Proof-of-Work :-

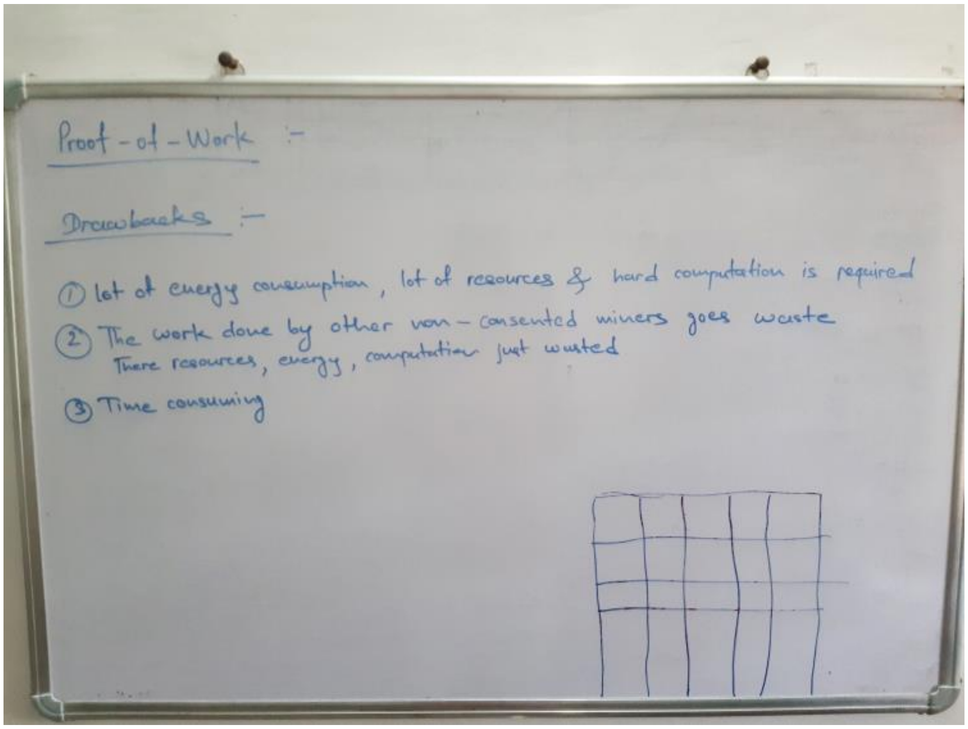
When a miner wants to add new block in blockchain, then following steps are required in POW,

1. Miners who want to add block has to solve a cryptographic puzzle
2. They have to do computation on there block header
3. In block header they know Timestamp, prevHash but do not know Nonce
4. They have to find Nonce correctly to solve puzzle
5. They select Nonce on trial-error basis & apply SHA-256 on block header
6. If that solved ans < Diffcultylevel then it proceeds further else again solve the puzzle
7. Now the correct value of Nonce found by miner is broadcasted into network & other miners gives consensus to that miner.
8. After that the miner can add the block in the network.



Proof-of-Work :-

Block header
Timestamp
Nonce
Prev hash
Apply SHA-256 to get correct value of Nonce
{ Ans < Difficultylevel }
A number predetermined by the network.
Proceed with broadcasting
A
B
C
D
E



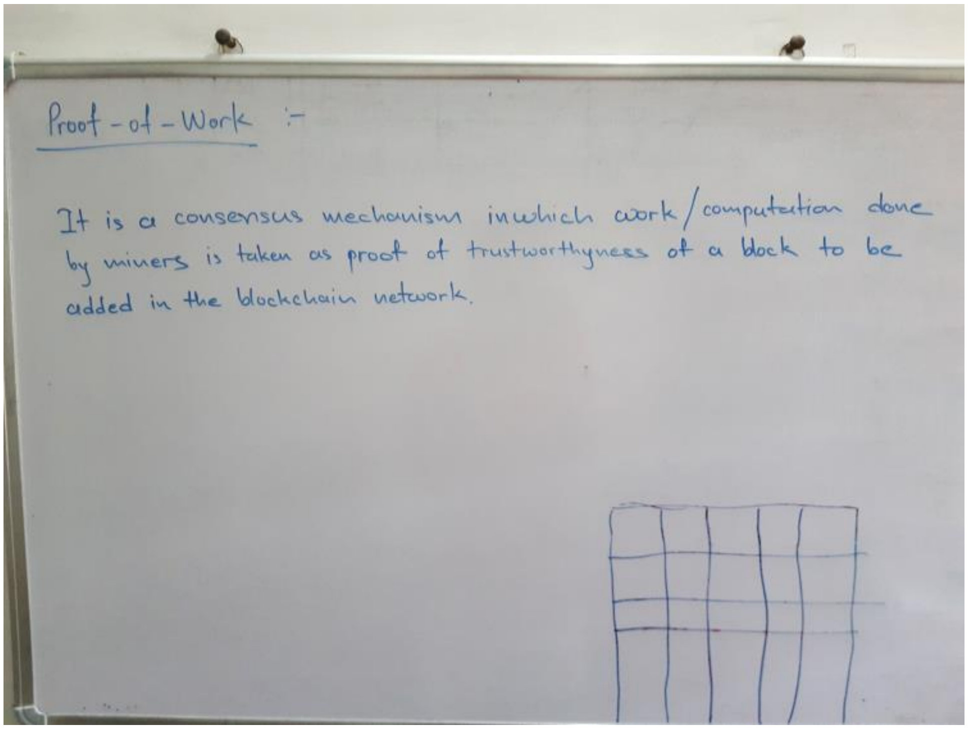
Proof-of-Work :-

Drawbacks :-

① lot of energy consumption, lot of resources & hard computation is required

② The work done by other non-consented miners goes waste
There resources, energy, computation just wasted

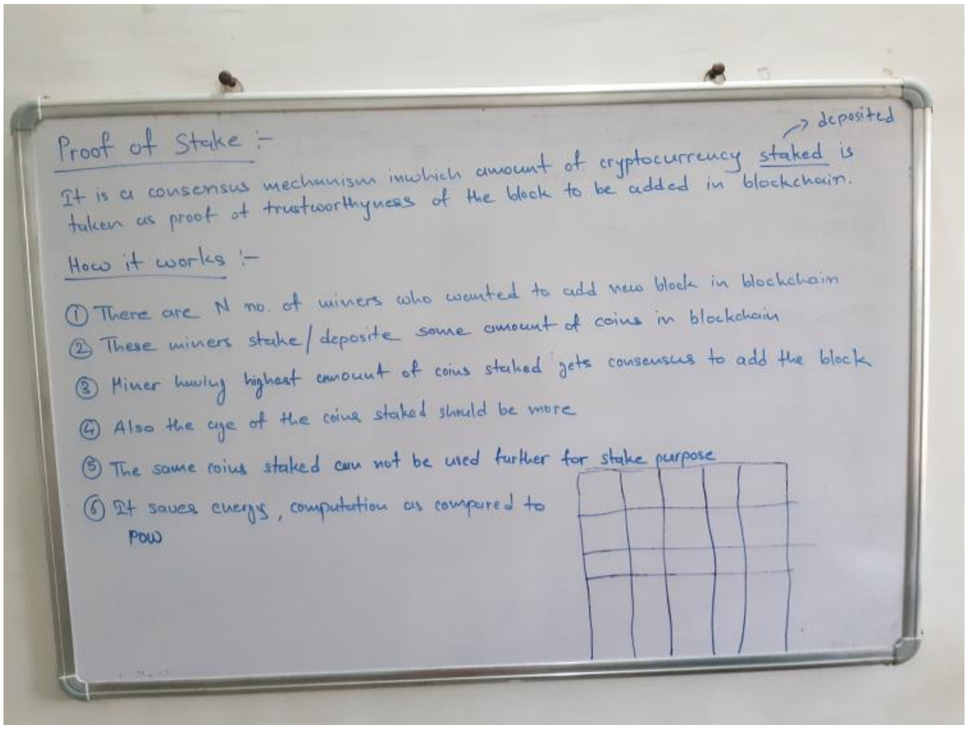
③ Time consuming



Proof-of-Work :-

It is a consensus mechanism inwhich work/computation done by miners is taken as proof of trustworthyness of a block to be added in the blockchain network.

PoS (Proof of Stake)-



## Proof of Stake :-

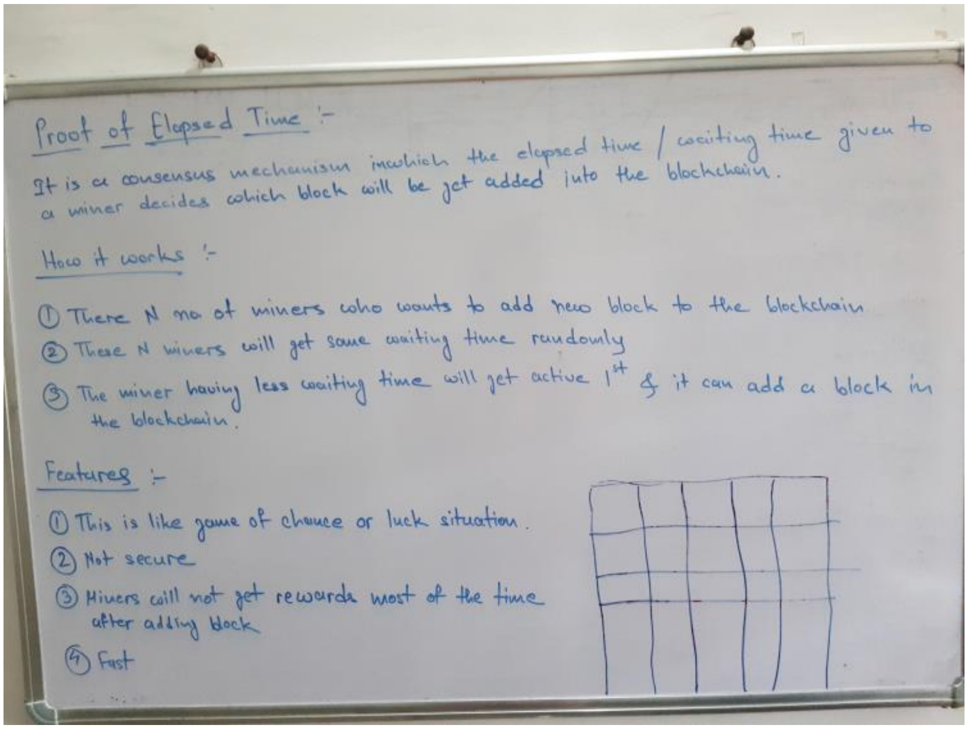
→ deposited

It is a consensus mechanism inwhich amount of cryptocurrency staked is taken as proof of trustworthyness of the block to be added in blockchain.

How it works :-

① There are N no. of miners who wanted to add new block in blockchain
② These miners stake / deposite some amount of coins in blockchain
③ Miner having highest amount of coins staked gets consensus to add the block
④ Also the age of the coins staked should be more
⑤ The same coins staked can not be used further for stake purpose
⑥ It saves energy, computation as compared to POW

PoET (Proof of Elapsed Time)-



## Proof of Elapsed Time :-

It is a consensus mechanism inwhich the elapsed time / waiting time given to a miner decides which block will be get added into the blockchain.

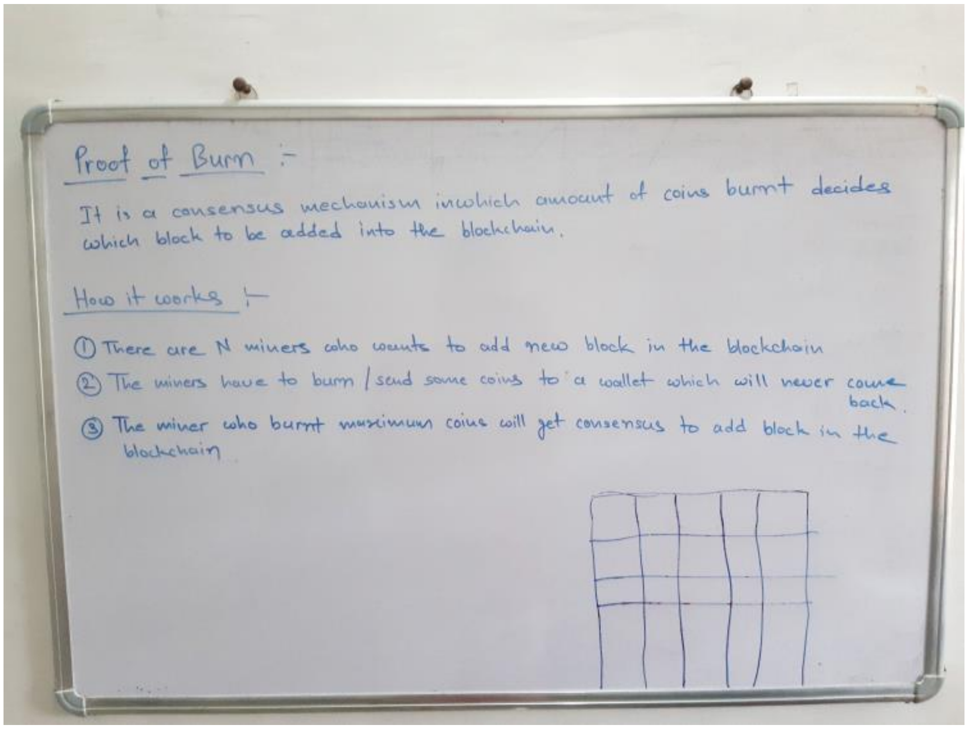
How it works :-

① There N no of miners who wants to add new block to the blockchain
② These N miners will get some waiting time randomly
③ The miner having less waiting time will get active 1st & it can add a block in the blockchain.

Features :-

① This is like game of chance or luck situation.
② Not secure
③ Miners will not get rewards most of the time after adding block
④ Fast

PoB (Proof of Burn)-



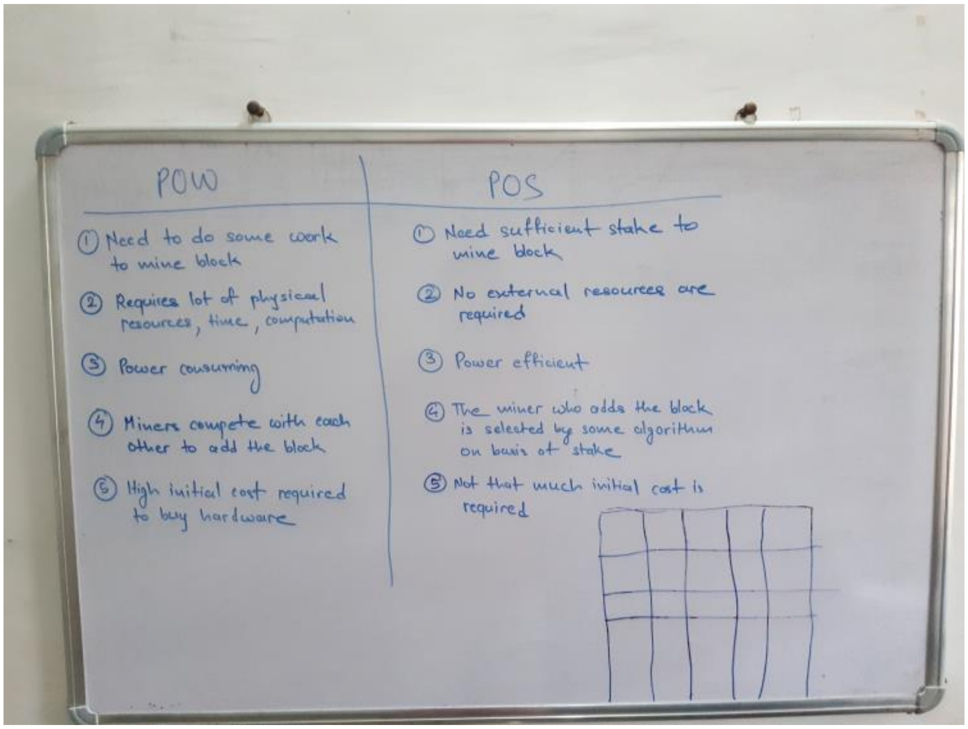
Proof of Burn :-

It is a consensus mechanism inwhich amount of coins burnt decides which block to be added into the blockchain.

How it works :-

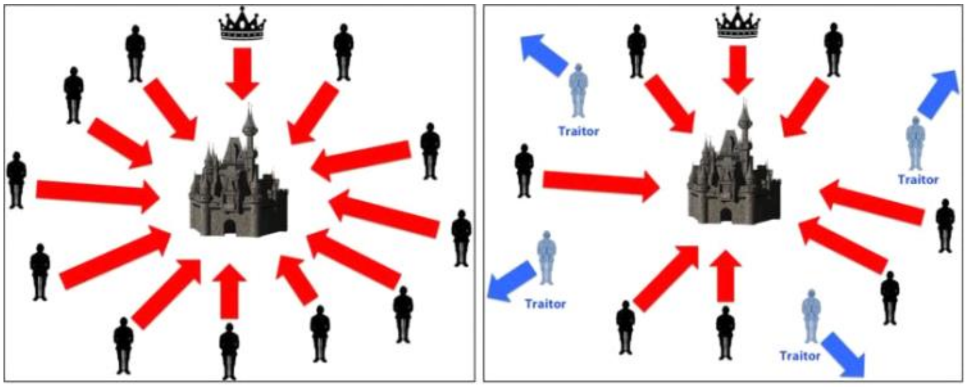
1. There are N miners who wants to add new block in the blockchain
2. The miners have to burn / send some coins to a wallet which will never come back.
3. The miner who burnt maximum coins will get consensus to add block in the blockchain

POW vs POS -

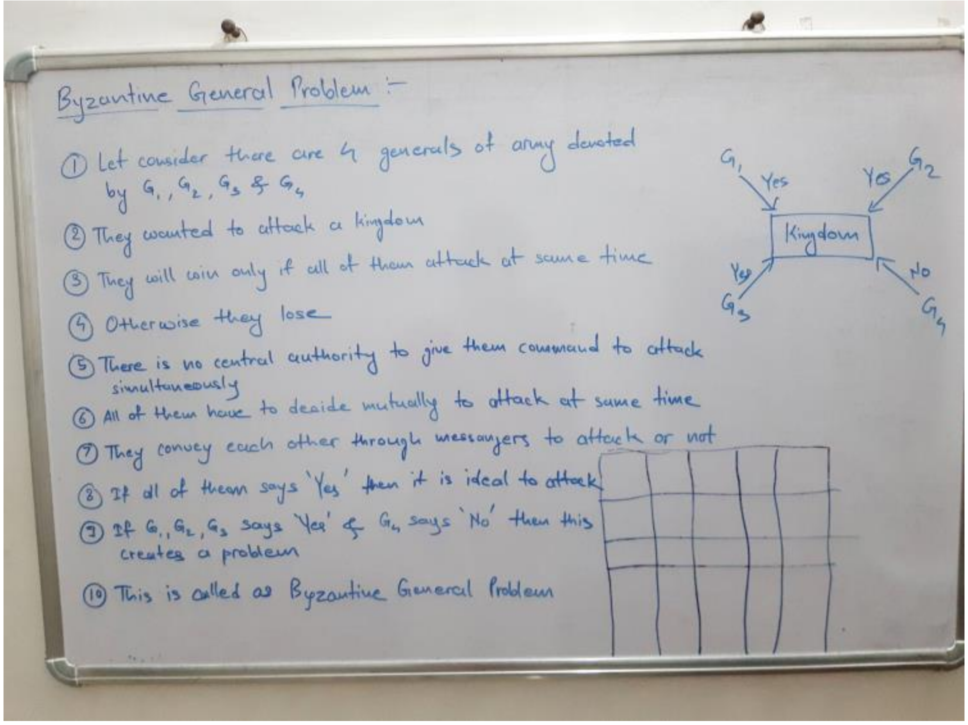


| POW | POS |
|---|---|
| 1. Need to do some work to mine block | 1. Need sufficient stake to mine block |
| 2. Requires lot of physical resources, time, computation | 2. No external resources are required |
| 3. Power consuming | 3. Power efficient |
| 4. Miners compete with each other to add the block | 4. The miner who adds the block is selected by some algorithm on basis of stake |
| 5. High initial cost required to buy hardware | 5. Not that much initial cost is required |

Byzantine General Problem -



**Coordinated Attack Leading to Victory** **Uncoordinated Attack Leading to Defeat**



Byzantine General Problem :-

① Let consider there are 4 generals of army devoted by $G_1$, $G_2$, $G_3$ & $G_4$

② They wanted to attack a kingdom

③ They will win only if all of them attack at same time

④ Otherwise they lose

⑤ There is no central authority to give them command to attack simultaneously

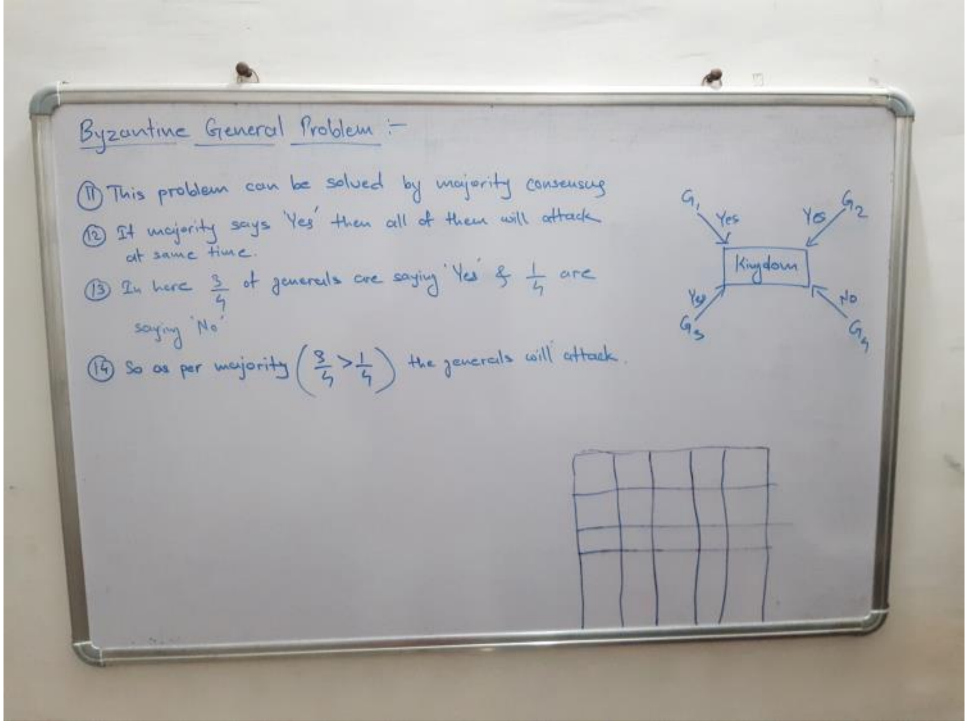
⑥ All of them have to decide mutually to attack at same time

⑦ They convey each other through messangers to attack or not

⑧ If all of them says 'Yes' then it is ideal to attack

⑨ If $G_1$, $G_2$, $G_3$ says 'Yes' & $G_4$ says 'No' then this creates a problem

⑩ This is called as Byzantine General Problem



## Byzantine General Problem :-

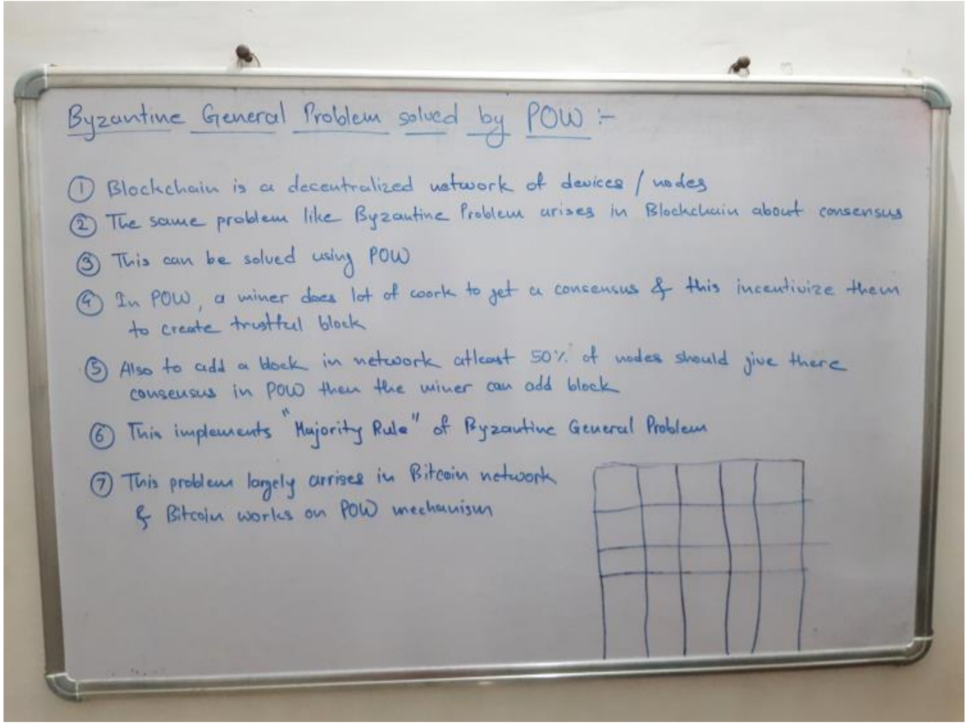
(11) This problem can be solved by majority consensus

(12) If majority says 'Yes' then all of them will attack at same time.

(13) In here $\frac{3}{4}$ of generals are saying 'Yes' & $\frac{1}{4}$ are saying 'No'

(14) So as per majority $\left(\frac{3}{4} > \frac{1}{4}\right)$ the generals will attack.

G1
Yes
Yes
G2
Kingdom
Yes
G3
No
G4



## Byzantine General Problem solved by POW :-

1. Blockchain is a decentralized network of devices / nodes
2. The same problem like Byzantine Problem arises in Blockchain about consensus
3. This can be solved using POW
4. In POW, a miner does lot of work to get a concensus & this incentivize them to create trustful block
5. Also to add a block in network atleast 50% of nodes should give there consensus in POW then the miner can add block
6. This implements "Majority Rule" of Byzantine General Problem
7. This problem largely arrises in Bitcoin network & Bitcoin works on POW mechanism