SMVS
Page No.
Date : / /

Permissioned Blockchain

* Consensus Algorithm in Permissioned Blockchain.

=> To achieve consensus across multiple blockchain, permissioned blockchain use different consensus protocols.

Permissioned Blockchain Consensus Algorithm

Synchronous Network	Asynchronous Network
- RAFT	- PBFT
- Paxos	
- BFT	

=> Synchronous Network:

In this network, all nodes are communicate with each other in a fixed, predicable time.

SMVS
Page No.
Date : / /

1 PAXOS :

PAXOS used For Handles Crash and Network Faults in the synchronous network.

PAXOS ensures a value is agreed upon even if some nodes fail or the network experiences issues.

It works by proposing values and reaching agreement through majority voting.

-> Process :

1 Proposers Propose a Value :

One or more proposer nodes suggest a value and every proposal has a unique number.

The proposers send their proposal to all the other node which called as Acceptors.

2 Acceptor accept or reject the proposal :

SMVS
Page No.
Date : / /

The acceptors compare the new proposal with the highest proposal they are already accepted.

If New proposal has a higher number than acceptor accepts it, else they reject it.

3 Learners learn the outcome:

Learners are nodes that observe the decisions made by the acceptors.

4 Consensus is reached:

When a majority of acceptors accept the same proposal, consensus is achieved.

2 RAFT

-> RAFT is simplifies consensus by using a leader-Follower Model.

In this model, Leader is chosen to manage decisions and the followers replicates its actions.

Page No.
Date : / /

-> Process:

1 Leader election:

All nodes in the system vote to elect one node as the leader.

2 Leader manages state replication:

The leader is responsible for proposing and replicating change to all the follower nodes.

3 Followers replicate leader's actions:

Followers don't make decisions on their own. They only respond to the leader's commands and replicate its action.

4 Handling Leader Failure:

IF followers stop receving the Leader's message than they assume the leader has failed.

The followers then initiates a new election to choose a new leader.

SMVS
Page No.
Date : / /

5 Consensus:

RAFT achieves consensus by ensuring that the leader replicates the same state to the majority of nodes.

3 BFT:

BFT stands For Byzantime Fault ensures consensus even when some nodes are faulty.

BFT is more robust than PAXOS and RAFT which only handles crashes and network issues.

-> Process:

1 Byzantime Generals Problem:

Imagine (~~Gervaral~~) several general trying to agree on a battle plan.

The honest general needs to agree on the same plan, even traitors are sending conflicting data.

SMVS
Page No.
Date : / /

2 Message-passing System:

Each node communicates with others by sending message.

Honest nodes will send correct message, while fauly nodes may send false message.

3 Consensus Rules:

BFT assumes that up to one-third of the nodes could be faulty.

For consensus to be achieved, at least 2/3 of nodes need to be honest

4 Decision Making:

They (~~Use~~) use a voting mechanism where they agree on the majority decision while ignoring faulty nodes data.

SMVS
Page No.
Date : / /

=> Asynchronous Network:

In Asynchronous network, Practical Byzantime Fault Tolerance provides consensus.

PBFT improves on traditional BFT by reducing energy consumption and offering finality.

PBFT works on the principle of state machine replication where one node act as leader and rest are secondary nodes.

-> Process of PBFT:

1 Request From Client:

The client initiates the process by sending the service request to the primary node.

2 Pre-prepare and Broadcast to Secondary Nodes:

Primary node receiving the request from the Client and the Node broadcasts the request to all the other node (Secondary).

Date : / /

This Secondary node receive the same request and expected to perform the same operation.

3 Nodes Performs Request and Respond:

Each node performs the requested operation and generates a result.

After that, All nodes are send their ~~rs~~ results directly back to the client.

4 Client Verifies Response:

The client receives responses from all the nodes.

If the majority of the responses are identical, the client concludes that the request has been successfully executed and the result is (~~id~~) Finalized.

SMVS
Page No.
Date : / /

* Crowd Funding:

=> Crowd Funding is a way to raise money for a new business by collecting small amounts of money from many people.

Blockchain eliminates the need of third-party intermediaries in the process of collecting the Funding.

It reduces costs by removing platform fee for collecting the Funde

-> How Blockchain Support Crowd Funding:

1 Decentralization: Blockchain eliminates reliance on third-party platforms and give the creators full control over their projects.

2 Equity Access via Tokenization: Asset tokenization allows investors to receive equity or ownership stake in a project using the blockchain.

Page No.
Date : / /

3 Global Accessibility: Anyone with an internet connection can invest in blockchain-based crowdfunding by enabling global participation.

4 Flexible Funding Options: Creators can issue custom tokens or digital currencies for fundraising.

5 Peer-to-Peer Transactions: Blockchain facilitates direct peer-to-peer cryptocurrency transaction which speed up the funding process.

* Byzantine Generals Problem:

=> The BGP describes a situation where multiple parties need to make a decision but face the communication challenges.

Some participants may send false or conflicting information which leads to potential failure.

SMVS
Page No.
Date : / /

The Goal is to a group of generals have to agree on a comman decision.

Between all the generals or parties coordination is essential for success.

The generals can only communicate through messengers, However some generals might send incorrect or misleading message.

This Faulty generals create a situation where it becomes hard to know who is truthful and who is not.

If some generals decide to attack while others decide to retreat, the ones who attack may lose because they don't have enough support.

For the army to win, all generals must take the same decision either attack or retreat.

If too many generals send false information, the group may fail to reach a coordinated decision.

* Supply Chain Management using Blockchain:

=> The Supply chain encompasses all activities involved in the production and distribution of goods.

Blockchain technology operates on a decentralized ledger where all the transaction are recorded in real time which help to see the all transaction scm.

Once a transation is recorded on the blockchain, it can not be altered or deleted which ensuring a permanent and transparent record of the supply chain history.

Blockchain allows the use of smart contract which automatically

SMVS
Page No.
Date : / /

execute transaction based on predefined condition.

-> This are the main component in the SCM in which Blockchain is used.

1 Raw Material Sourcing:

The process begins when a supplier provides raw materials and Each transaction is recorded on Blockchain

Blockchain records like the source, quality and quantity of raw material.

2 Manufacturing:

As the raw material move into production, the manufacturer updates the Blockchain with information such as batch number, production date etc.

3 Transportation and Logistics:

When the goods are shipped, the Blockchain is updated with

real-time data on the shipment's location, shipping method etc.

4 Warehousing:

Upon arrival at warehouse, the blockchain is updated to reflect the good's receipt.

All parties involved can access real-time data on stock levels.

5 Retail and Customer Delivery:

When goods move from the warehouse to the retailer the blockchain records the transfer of ownership.

For end customers, Blockchain provides real-time tracking of the delivery.