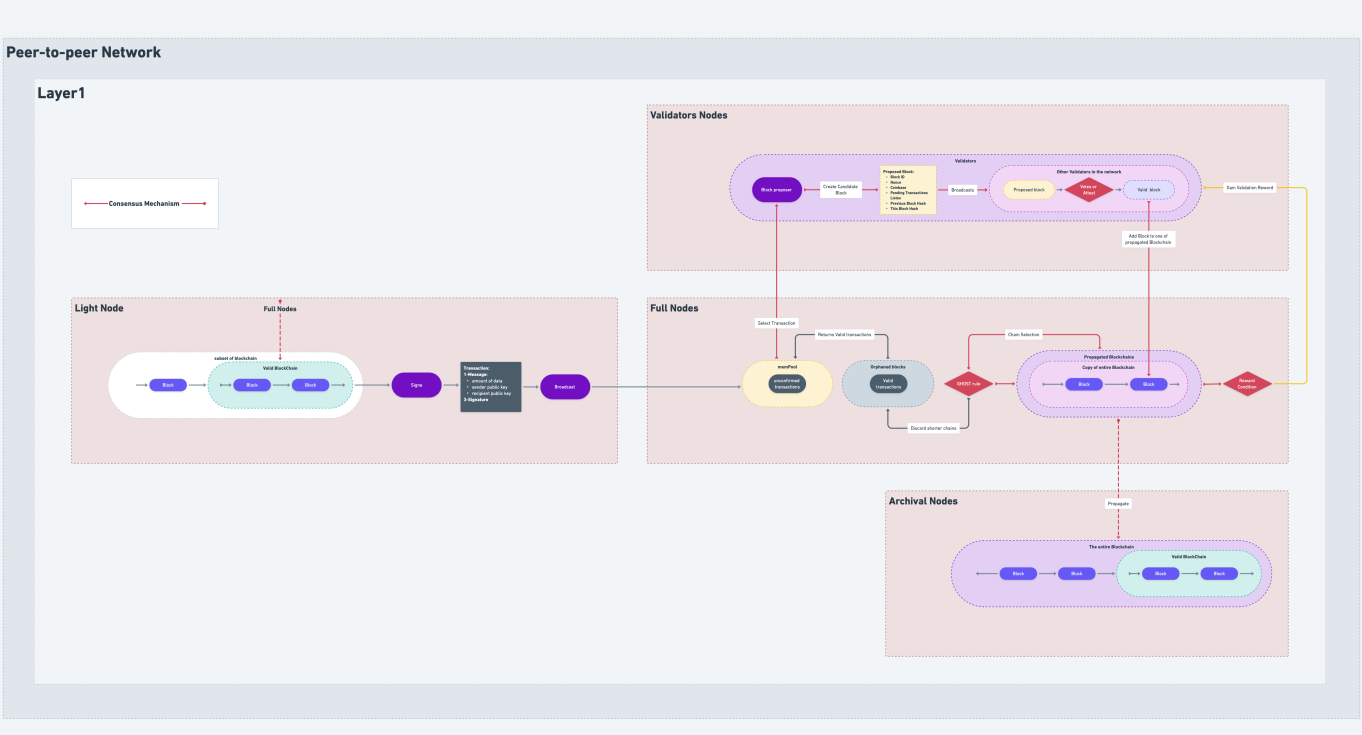
Blockchain Consensus Mechanisem

Proof of work with Longest Chain Rule.

By Yaakoub Belhardi / Quinn Future CTO



1. Light Nodes or Wallets:

Generate a Transaction:
The user creates a transaction, such as transferring tokens, deploying a contract, or invoking a smart contract.

Sign the Transaction:
The transaction is signed with the user's private key to ensure authenticity and integrity.

Broadcast to the Network:
The signed transaction is sent to the L1 network, where it enters the mempool (a queue of pending transactions).

2. Full Nodes (Mempool):

Transaction Pooling:
All unprocessed transactions are stored in the mempool, waiting to be included in a block.

Prioritization:
Miners or validators prioritize transactions based on factors like gas fees (in Proof of Work) or stake and reputation (in Proof of Stake).

3. Validators Nodes (Consensus Mechanism):

Select Transactions:
Miners/validators select transactions from the mempool, typically prioritizing those with higher fees.

Validate Transactions:

They verify:
Signature Validity: Ensures the transaction was signed by the sender.

Account Balance: Checks if the sender has sufficient funds or gas to cover the transaction and fees.

Smart Contract Rules: If the transaction interacts with a smart contract, it validates whether it adheres to the contract's logic.

Execute Transactions:
The node executes the transaction, updating the blockchain's state.

Prepare a Block:
Valid transactions are grouped into a candidate block.

4. Full Nodes (Consensus Mechanism):

Block Validation:

In Proof of Work (PoW): Miners solve a cryptographic puzzle to propose a valid block.

In Proof of Stake (PoS): Validators are chosen based on their stake to propose and validate the block.

Block Propagation:
The new block is broadcast across the network, where other nodes verify its validity.

Validate Block and Transactions:
Full nodes independently verify the new block and all included transactions.

Update Blockchain State:
Once validated, the block is added to the blockchain, updating the global state, such as account balances and contract states.

Finality:
A transaction is considered confirmed once it is included in a block and additional blocks are built on top (to reduce the risk of reorganization).

Global State Update:
The transaction's effect (e.g., a token transfer) is reflected in the blockchain's global state.

5. Archival Nodes:

Propagate canonical Blockchain:
Full nodes propagate and update the L1 Archival blockchain to the canonical L1 blockchain.

6. Light Nodes or Wallets:

Propagate canonical Blockchain:
Full nodes propagate and update the Subset of blockchain to the canonical L1 blockchain.