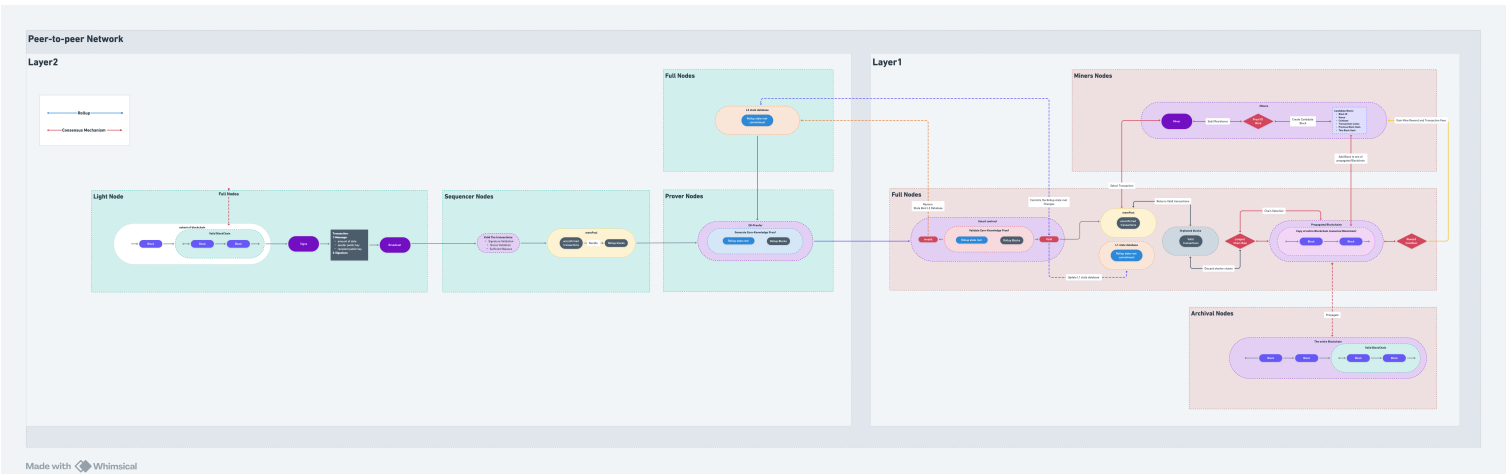
Blockchain Consensus Mechanisem

Proof of work with Longest Chain Rule, ZK-Rollup

By Yaakoub Belhardi / Quinn Future CTO



1. L2 Light Nodes or Wallets:

Generate a Transaction:
A user creates a transaction, such as transferring tokens or calling a smart contract on L2.

Sign the Transaction:
The transaction is signed using the sender's private key to ensure authenticity and prevent tampering.

Send to L2 Sequencer Nodes:
The signed transaction is forwarded to L2 Sequencer Nodes for processing.

2. L2 Sequencer Nodes:

Collect and Order Transactions:
The sequencer collects transactions from various users, orders them, and groups them into batches.
These batches improve scalability by reducing the frequency of interactions with L1.

Send to Prover Nodes:
The sequencer sends the batched transactions to L2 Prover Nodes for further processing.

3. L2 Prover Nodes:

Process Transactions:
The prover nodes execute all transactions in the batch, computing the new state transitions for the L2 system.

Generate Zero-Knowledge Proof (zk-Proof):
After processing the transactions, the prover generates a zk-proof.
The zk-proof cryptographically proves the validity of the transactions and the resulting state transitions without revealing sensitive information.

Send zk-Proof and State to L1:
The prover sends the transaction batch, zk-proof, and updated state root commitment to the L1 smart contract for validation.

4. L1 Smart Contract:

Validate zk-Proof:
The L1 smart contract verifies the zk-proof. If the proof is valid, this confirms that all transactions in the batch and the resulting state transitions are correct.

Commit New State Root:
The L1 smart contract updates the state root of the L2 rollup system, representing the latest state after processing the transactions.

Pass Valid Transactions to Mempool:
After zk-proof validation, valid transactions are passed to the L1 mempool for inclusion in an L1 block.

5. L1 Miners Nodes:

Select Transactions from Mempool:
Miners pick transactions from the mempool, including zk-rollup-related updates, to include in a new block.

Proof of Work (PoW) or Sybil Resistance Mechanism:
Miners perform computational work (in PoW systems) or validate transactions according to the consensus mechanism (e.g., PoS in Ethereum 2.0).

Create Candidate Block:
Miners prepare a candidate block containing the zk-rollup transactions and other network transactions.

Add Block to Blockchain:
The new block is added to the blockchain and propagated across the network, updating all full nodes with the new state.

6. Full Nodes:

Longest Chain Rule:
Full nodes maintain the entire L1 blockchain and select the longest valid chain as the canonical chain.

Discard Orphaned Blocks:
Shorter or invalid chains (orphaned blocks) are discarded, ensuring consistency across the network.

7. Archival Nodes:

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

8. L2 Light Nodes or Wallets:

Propagate canonical Blockchain:
Full nodes propagate and update the L2 Subset of blockchain to the canonical L1 blockchain.