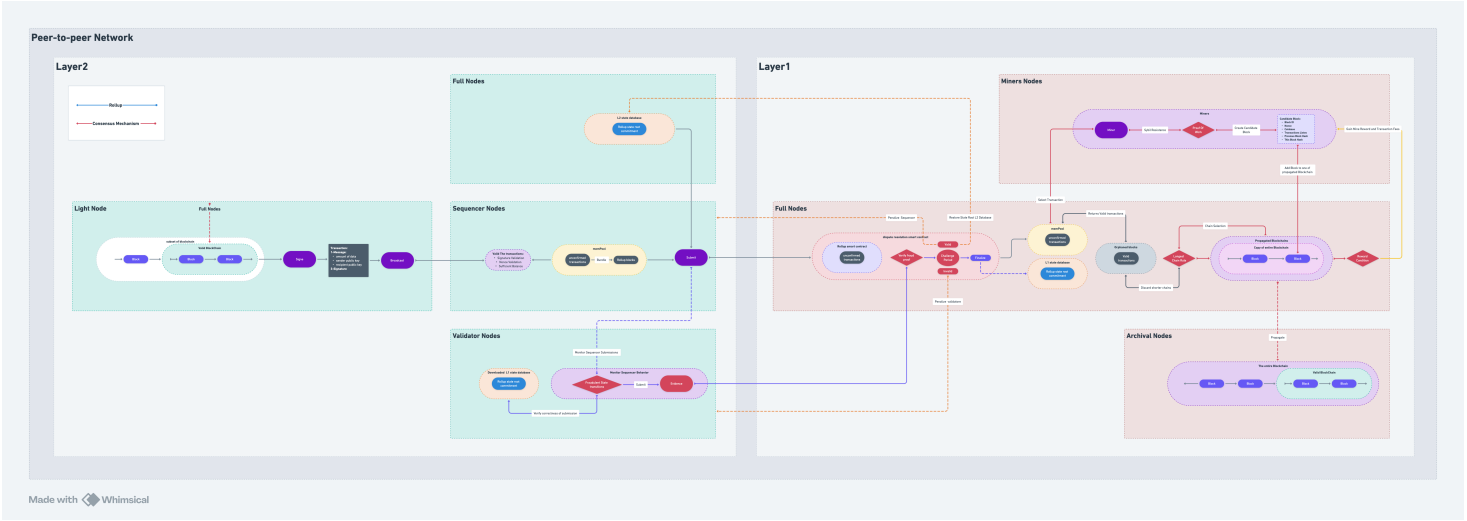
Blockchain Consensus Mechanisem

Proof of work with Longest Chain Rule, Optimistic Rollup

By Yaakoub Belhardi / Quinn Future CTO



1. L2 Light Nodes or Wallets:

Generate a Transaction:
A user initiates a transaction, such as transferring tokens or interacting with an L2 smart contract.

Sign the Transaction:
The transaction is signed using the user's private key for security and authenticity.

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

2. L2 Sequencer Nodes:

Collect and Order Transactions:
Sequencer nodes collect transactions from users, order them into batches, and execute them locally to compute the updated state transitions.

Submit State Commitment to L1:
Instead of providing cryptographic proofs like zk-proofs, the sequencer submits the state root commitment of the updated L2 system to the L1 smart contract. This submission assumes transactions are valid (hence the term "optimistic").

Broadcast Transactions and Batch Details:
The sequencer broadcasts the transaction details to other L2 nodes for replication and ensures transparency.

3. L2 Validators or Watchers Nodes:

Monitor Transactions:
Validators or watchers monitor the transactions and state commitments submitted by the sequencer to L1.

Challenge Period:
A challenge period is set on L1. During this period, validators can challenge fraudulent state transitions by submitting a fraud proof to the L1 smart contract. Fraud proofs typically re-execute the disputed transaction or batch on L1 to verify its validity.

Resolve Disputes:
If the fraud proof proves invalidity, the malicious batch is rejected, and penalties are applied to the sequencer. If no challenges arise during the challenge period, the state is considered finalized.

4. L1 Smart Contract:

Receive State Commitment:
The L1 smart contract stores the state root commitment sent by the sequencer.

Handle Challenges:
The contract processes fraud proofs submitted by validators, either confirming or rejecting the disputed state.

Finalize State Root:
After the challenge period, the state root is finalized if no valid fraud proof is submitted.

Pass Valid Transactions to Mempool:
Valid transactions are passed to the L1 mempool for inclusion in an L1 block.

5. L1 Miners Nodes:

Select Transactions from Mempool:
Miners (in PoW) or validators (in PoS) include optimistic rollup-related state updates in L1 blocks.

Create Candidate Blocks:
The rollup state updates are incorporated into L1 candidate blocks, propagating the data across the network.

Add Blocks to Blockchain:
These blocks are added to the L1 blockchain and synchronized across all L1 full nodes.

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.