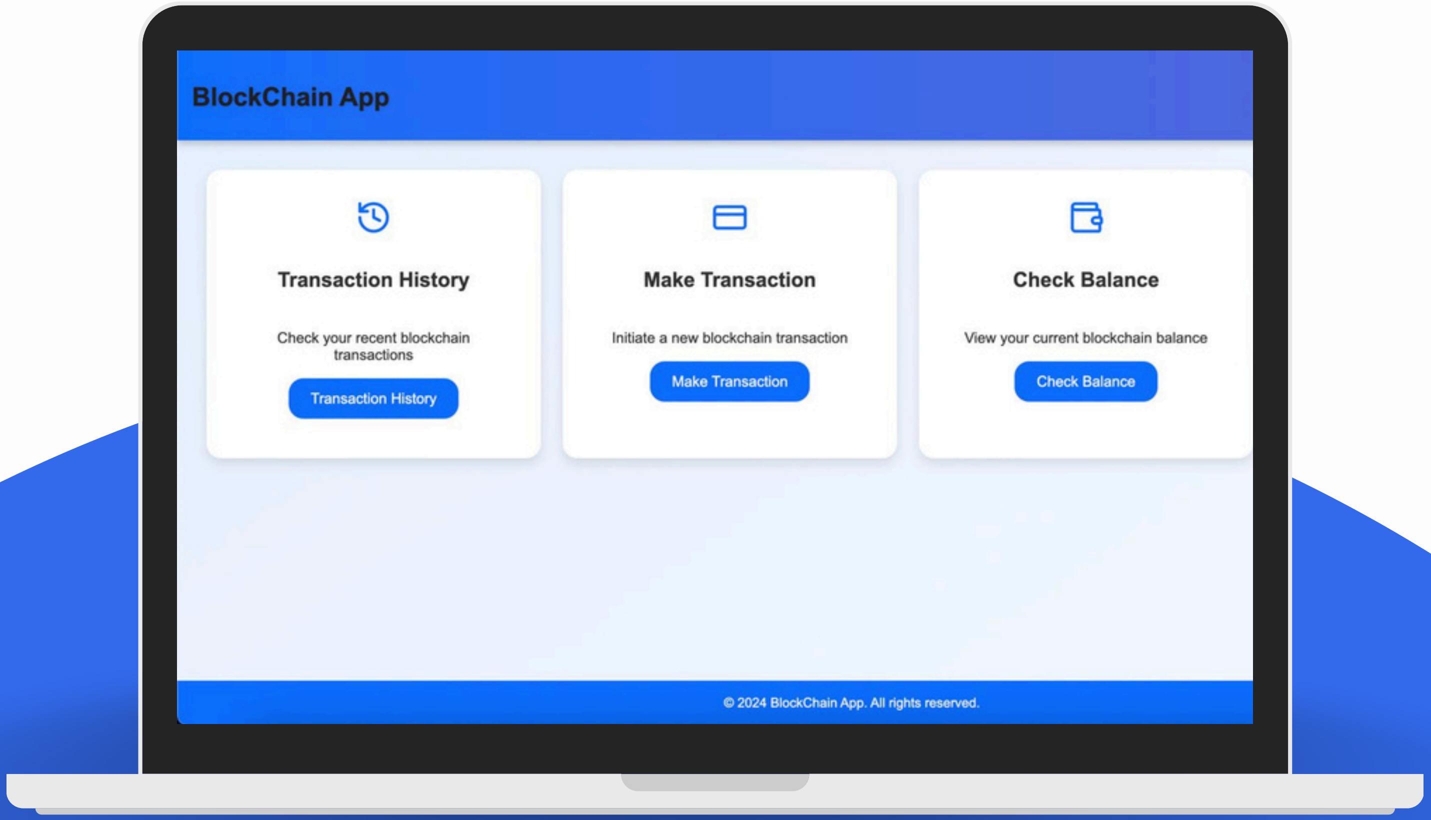
CRYPTONIX

BLOCKCHAIN IMPLEMENTATION WITH MERKLE TREE

CSL2020



BlockChain App

Transaction History

Check your recent blockchain transactions

Make Transaction

Initiate a new blockchain transaction

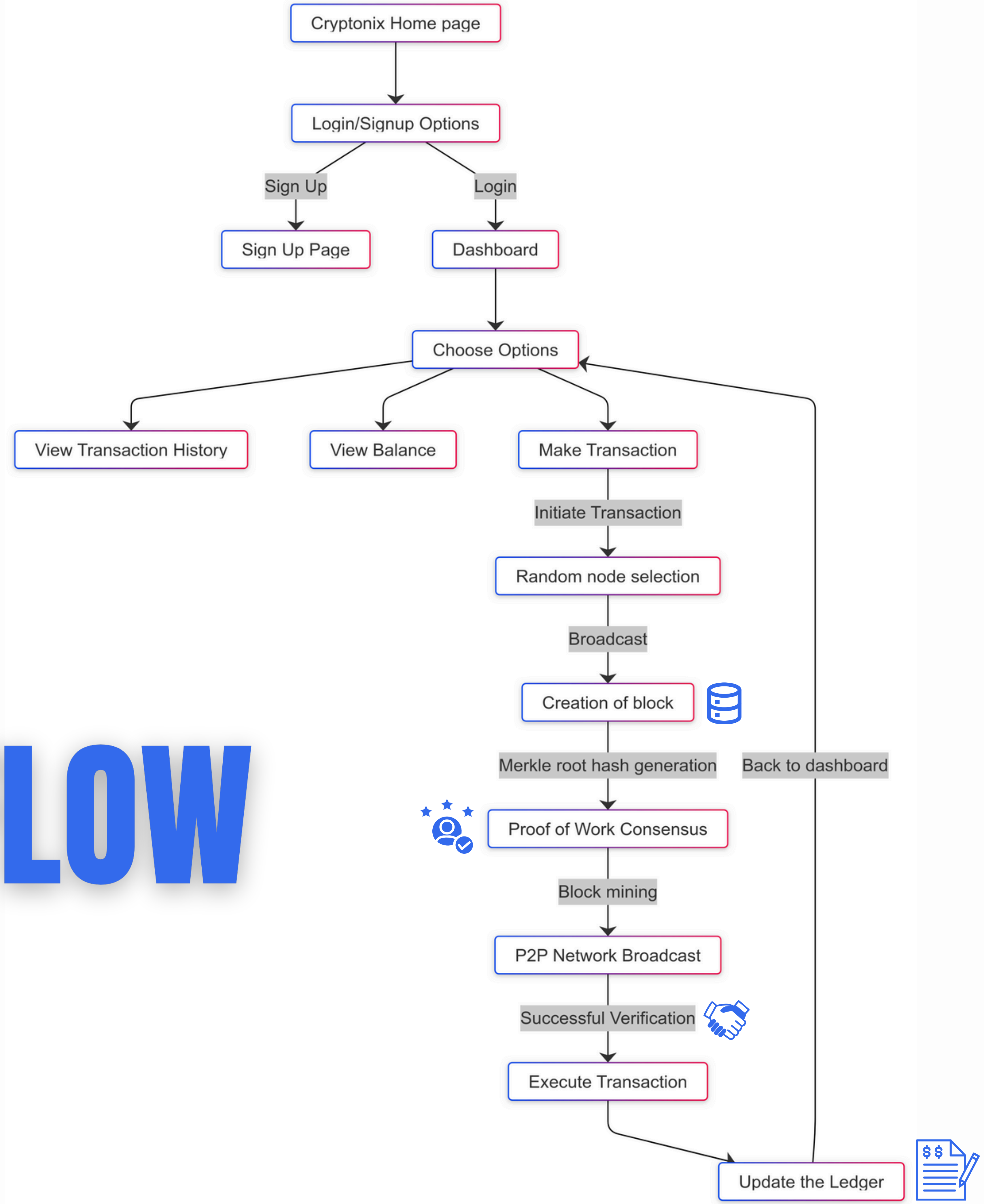
Check Balance

View your current blockchain balance

© 2024 BlockChain App. All rights reserved.

Sahil Narkhede | Rishi Kaneria | Saher Dev
Sahilpreet Singh | Akshay Sake
Mentor - Prajjwal Nijhara

WORKFLOW



Cryptonix Home page

Login/Signup Options

Sign Up

Login

Sign Up Page

Dashboard

Choose Options

View Transaction History

View Balance

Make Transaction

Initiate Transaction

Random node selection

Broadcast

Creation of block

Merkle root hash generation

Back to dashboard

Proof of Work Consensus

Block mining

P2P Network Broadcast

Successful Verification

Execute Transaction

Update the Ledger

MERKLE TREE IMPLEMENTATION

01

Merkle Tree Implementation

Each block uses a Merkle tree to organize and hash all transactions, generating a unique Merkle root.

02

Merkle Root Storage

The Merkle root for each block's transactions is stored directly in the block header.

03

Chained Merkle Roots

Each new block computes its own Merkle root, combining it with the Merkle root of the previous block. This chained approach links block integrity, securing the continuity of transaction data across blocks.

04

Enhanced Security

The combined Merkle root structure makes tampering with any block data detectable, enhancing data integrity and security in the blockchain.

PROOF OF WORK

01

Mining Process
Miners compete to find a valid solution, of finding a hash below a certain target (difficulty level). This process ensures that only valid blocks are added, making it resistant to tampering.

02

Block Validation
Once a miner solves the puzzle, the new block, along with its valid hash, is broadcast to the network. Other nodes verify the solution before accepting the block and adding it to their copy of the blockchain.

03

Security and Integrity
The PoW algorithm makes it computationally impractical for any malicious actor to alter previous blocks because altering any block would require recalculating the PoW for all subsequent blocks.

04

Decentralization and Trust:
PoW allows the blockchain to function decentralized, with no central authority required to validate transactions. Miners and nodes reach a consensus through computational effort, maintaining trust in the blockchain network.

P2P NETWORK

01

P2P Network Architecture
The blockchain uses a decentralized peer-to-peer (P2P) network to enable nodes (users/verifiers) to connect and communicate directly.

02

Transaction Broadcasting
When a new transaction is created, it is broadcast across the P2P network to reach all connected nodes. Each node receives the transaction, verifying its authenticity before further propagation.

03

User Verification
Upon receiving a transaction, nodes act as verifiers to confirm transaction validity. Verified transactions are then stored in each node’s memory pool, awaiting inclusion in a new block.

04

Consensus and Synchronization
The P2P network allows nodes to reach consensus, ensuring that only validated transactions are added to the blockchain. It enables all nodes to maintain an updated, consistent copy of the blockchain ledger.

TIME-COMPLEXITY ANALYSIS

Merkle Root	$O(nlogn)$
Proof of Work	$O(2^d)$
Block Addition	$O(nlogn+2^d)$
Total Blockchain	$O(b \cdot (nlogn+2^d))$

THANK YOU!