CLAIMS

1. A computer-implemented method for communicating shared blockchain data, the method comprising:

sending, by a consensus node of a blockchain network, current state information and one or more transactions associated with a current block of a blockchain to one or more shared storage nodes of the blockchain network, wherein the consensus node stores block header associated with every block of the blockchain and the current state information, the one or more shared storage nodes store block body and historic state information associated with every block of the blockchain, and wherein the historic state information is stored as key-value pairs (KVPs) of a historic state tree with values being account states of accounts associated with the blockchain network and keys being hash values of the corresponding account states;

verifying, by the consensus node, that the one or more transactions are stored by the one or more shared storage nodes; and

receiving, by the consensus node from one of the one or more shared storage nodes, a notification of a transaction associated with the consensus node,

wherein the one or more shared storage nodes are elected by receiving 2f + 1 votes from all 3f + 1, 3f + 2, or 3f + 3 nodes of the blockchain network, and wherein f is the maximum number of faulty shared storage nodes and consensus nodes that can be tolerated within the blockchain network.

2. The computer-implemented method of claim 1, wherein verifying the one or more transactions are stored by the one or more shared storage nodes are performed based on simplified payment verification.

3. The computer-implemented method of any previous claim, wherein sending the current state information further comprises sending the current state information and a hash value of the current state information as KVP to the one or more shared storage nodes of the blockchain network.

4. The computer-implemented method of any previous claim, wherein the current state information and the one or more transactions sent by the consensus node includes a digital signature generated based on a private key associated with the consensus node.

5. The computer-implemented method of any previous claim, further comprises:

sending, by the consensus node, a hash value to the one of the one or more shared storage nodes for retrieving an account state stored in the historic state tree;

receiving, by the consensus node, the account state in response to sending the hash value; and

verifying, by the consensus node, that the account state is part of the blockchain based on the hash value.

6. The computer-implemented method of any preceding claim, wherein the blockchain network includes at least f + 1 shared storage nodes and no more than 2f + 2 consensus nodes.

7. The computer-implemented method of any preceding claim, wherein a current state tree includes KVPs with values being account sates associated with the current block and keys being node IDs corresponding to nodes of the current state tree and a block ID corresponding to the current block.

8. The computer-implemented method of any preceding claim, wherein verifying that the account state is part of the blockchain is performed based on hashing the account state to generate a hashed account state and comparing the hashed account state to the hash value.

9. The computer-implemented method of claim 7, wherein the current state tree and the historic state tree are stored as a fixed depth Merkle tree.

10. A system communicating shared blockchain data, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 9.

11. An apparatus for communicating shared blockchain data, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 9.