

CLAIMS

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

determining, by a blockchain node of a blockchain network, block data and current state data associated with a current block of a blockchain;

sending, by the blockchain node, the current state data to one or more shared storage nodes of the blockchain network, wherein the blockchain node stores the current state data and the one or more shared storage nodes store historic state data associated with every block of the blockchain;

performing, by the blockchain node, error correction coding of the block data to generate encoded block data, wherein the error correction coding is configured to recover missing bits of original data using the encoded block data;

dividing, by the blockchain node based on one or more predetermined rules, the encoded block data into a plurality of data sets, wherein the one or more predetermined rules provide an equal distribution of data sets between the shared storage nodes;

storing, by the blockchain node based on the one or more predetermined rules, one or more data sets that form a portion of the plurality of data sets;

hashing, by the blockchain node, each data set of remaining data sets of the plurality of data sets to generate one or more hash values corresponding to the remaining data sets; and

storing, by the blockchain node, the one or more hash values and the current state data.

2. The computer-implemented method of claim 1, further comprising:

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

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

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

3. The computer-implemented method of claim 1, wherein the blockchain network includes at least $f + 1$ shared storage nodes and no more than $2f + 2$ consensus nodes, and wherein f is a maximum number of faulty shared storage nodes and consensus nodes that can be tolerated within the blockchain network.

4. The computer-implemented method of claim 1, 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 a maximum number of faulty shared storage nodes and consensus nodes that can be tolerated within the blockchain.

5. The computer-implemented method of claim 1, wherein the current state data and the historic state data are stored as a fixed depth Merkle tree.

6. The computer-implemented method of claim 1, wherein the error correction coding is erasure coding.

7. The computer-implemented method of claim 1, wherein the blockchain node is a first blockchain node, and further comprising:

determining that at least a portion of the block data needed for executing a smart contract is not stored by the first blockchain node;

identifying, based on the one or more predetermined rules, a second blockchain node that stores at least one data set of the remaining data sets of the plurality of data sets and at least one hash value corresponding to the at least one data set of the remaining data sets of the plurality of data sets; and

sending the at least one hash value to the second blockchain node for retrieving the at least one data set of the remaining data sets of the plurality of data sets.

8. The computer-implemented method of claim 7, wherein the at least one hash value is first at least one hash value, and further comprising:

receiving, from the second blockchain node, at least one data set in response to sending the first at least one hash value;

hashing the at least one data set to generate a second at least one hash value; and

determining that the at least one data set is authentic if the first at least one hash value is same as the second at least one hash value.

9. The computer-implemented method of claim 8, further comprising:

identifying, based on the one or more predetermined rules, a third blockchain node that stores at least one data set of the remaining data sets of the plurality of data sets and third at least one hash value corresponding to the at least one data set of the remaining data sets of the plurality of data sets;

sending the third at least one hash value to the third blockchain node for retrieving the at least one data set of the remaining data sets of the plurality of data sets;

receiving, from the third blockchain node, at least one data set in response to sending the third at least one hash value;

hashing the at least one data set to generate fourth at least one hash value; and

determining that the at least one data set is authentic if the third at least one hash value is same as the fourth at least one hash value.

10. The computer-implemented method of claim 1, wherein the one or more predetermined rules include one or more instructions for dividing the encoded block data to the plurality of data sets based on a quantity of blockchain nodes of a blockchain network and assignments of one or more data sets of the plurality of data sets to be stored or hashed by each blockchain node of the quantity of blockchain nodes.

11. The computer-implemented method of claim 1, further comprising:

storing the current block as a write-ahead log (WAL) file; and

reporting that the current block is stored and ready for consensus.

12. The computer-implemented method of claim 1, further comprising:
storing the block data in a buffer of the blockchain node, and wherein the error correction coding is performed in response to identifying that the buffer is full.
13. A system communicating shared blockchain data, comprises:
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 computer-implemented method of any of claims 1 to 12.
14. An apparatus for communicating shared blockchain data, the apparatus comprises a plurality of modules for performing the computer-implemented method of any of claims 1 to 12.