

CLAIMS

1. A computer-implemented method for storing blockchain data, the method comprising:
determining, by a blockchain node, one or more blocks that are infrequently visited,
wherein the one or more blocks are stored on the blockchain node and created on a blockchain;
performing, by the blockchain node, error correction coding of the one or more blocks to generate one or more encoded blocks;
dividing, by the blockchain node based on one or more predetermined rules, each of the one or more encoded blocks to a plurality of data sets;
selecting, by the blockchain node, one or more data sets from the plurality of data sets of each of the one or more encoded blocks based on the one or more predetermined rules;
hashing, by the blockchain node, the one or more data sets to generate one or more hash values corresponding to the one or more data sets;
storing, by the blockchain node, the one or more hash values; and
deleting, by the blockchain node, the one or more data sets.
2. The method of any previous claim, wherein the one or more blocks are determined as infrequently visited if the one or more blocks are created for a predetermined amount of time or no block data associated with the one or more blocks are retrieved to execute a smart contract for a predetermined amount of time.
3. The method of any previous claim, wherein the error correction coding is performed when utilization rate of computational resource of the blockchain node is less than or equal to a predetermined value or usage of storage space of the blockchain node is greater than or equal to a predetermined percentage.
4. The method of any previous claim, wherein the error correction coding is performed by adding redundant bits to the one or more blocks.
5. The method of any previous claim, wherein the error correction coding is erasure coding.

6. The method of any previous claim, wherein the blockchain node is a first blockchain node, and the method further comprising:

after deleting the one or more data sets, determining that block data needed for executing a smart contract is associated with at least one of the one or more data sets deleted by the first blockchain node;

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

sending the at least one hash value to the second blockchain node for retrieving the at least one of the one or more data sets.

7. The method of claim 6, wherein the at least one hash value is first at least one value, the method further comprising:

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

hashing the at least one data set to generate the second at least one hash value.

8. The method of claim 7, further comprising:

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

9. The method of claim 7, further comprising:

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

sending the third at least one hash value to the third blockchain node for retrieving the at least one of the one or more 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 a 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 the same as the fourth at least one hash value.

10. The method of any previous claim, further comprising:

before the deleting the one or more data sets, indexing the one or more hash values with a block ID of a corresponding block of the one or more blocks associated with the one or more hash values.

11. The method of any previous claim, wherein the one or more predetermined rules include one or more instructions for dividing the encoded blocks 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 of the blockchain nodes.

12. 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 11.

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