

CLAIMS

1. A computer-implemented method for storing keys of a plurality of key-value pairs in a network node of a blockchain network, the method comprising:

maintaining data representing a forest that stores a plurality of keys of the plurality of key-value pairs that are stored in a map, the forest comprising a plurality of trees, each tree comprising a respective plurality of storage nodes, each storage node storing a subset of the plurality of keys;

receiving a request to add a key of a key-value pair into the forest, the key-value pair stored in the map;

computing a first hash value of the key using a first hash function;

determining one of the plurality of trees to store the key based on the first hash value;

determining a target storage node of the one of the plurality of trees to store the key;

and

storing the key in the target storage node.

2. The method of claim 1, wherein the determining one of the plurality of trees to store the key based on the first hash value comprises:

performing a modulo operation on the first hash value to generate a first modulo value; and

determining the one of the plurality of trees to store the key based on the first modulo value.

3. The method of any preceding claim, wherein each of the plurality of trees comprises a respective number of levels, each level corresponding to a respective hash function.

4. The method of any preceding claim, wherein the one of the plurality of trees comprises a first level that comprises a root node, and the determining a target storage node of the one of the plurality of trees to store the key comprises:

determining whether the root node has available space for storing the key; and

in response to determining that the root node in the first level has available space for storing the key, storing the key in the root node in the first level, wherein the root node is the target storage node.

5. The method of any preceding claim, wherein the one of the plurality of trees comprises a first level that comprises a root node, and the determining a target storage node of the one of the plurality of trees to store the key comprises:

determining whether the root node has available space for storing the key; and

in response to determining that the root node in the first level does not have available space for storing the key,

computing a second hash value of the key using a second hash function, the second hash function corresponding to a second level of the one of the plurality of trees, the second hash function being different from the first hash function; and

determining the target storage node in the second level of the one of the plurality of trees to store the key based on the second hash value.

6. The method of claim 5, wherein determining the target storage node in the second level of the one of the plurality of trees to store the key based on the second hash value comprises:

performing a modulo operation on the second hash value to generate a second modulo value;

determining a second storage node in the second level of the one of the plurality of trees to store the key based on the second modulo value;

determining whether the second storage node has available space for storing the key; and

in response to determining that the second storage node in the second level has available space for storing the key, storing the key in the second storage node in the second level, wherein the second storage node is the target storage node.

7. The method of any preceding claim, wherein:

each tree of the plurality of trees comprises a plurality of leaf storage nodes and one or more non-leaf storage nodes, each of the one or more non-leaf storage nodes corresponding to a configurable number of child nodes, and

each storage node of the forest stores a configurable number of keys.

8. An apparatus for implementing a blockchain-based key storing system, the apparatus comprising a plurality of modules for performing the computer-implemented method of any one of claims 1 to 7.

9. A blockchain-based key storing system, 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 computer-implemented method of any one of claims 1 to 7.