

Claims

1. A data storage method, comprising:
 - sending, by a blockchain node associated with a blockchain, data to an encryption device to cause the encryption device to encrypt the data and return the encrypted data to the blockchain node;
 - receiving the encrypted data returned by the encryption device; and
 - sending the encrypted data to other blockchain nodes associated with the blockchain to cause each of the other blockchain nodes to store the encrypted data in the blockchain after performing consensus verification on the encrypted data with success.
2. The method according to claim 1, further comprising:
 - determining a first value corresponding to the data through a smart contract, the first value being used to represent a value added into an account of the blockchain node; and
 - sending the blockchain node's own node identifier and the first value to the other blockchain nodes to cause the node identifier and the first value to be stored in the blockchain after a consensus verification on the node identifier and the first value by the blockchain nodes passed.
3. The method according to claim 1, wherein the encryption device is caused to encrypt a part of the data.
4. The method according to claim 1, further comprising:
 - determining, by one of the blockchain nodes associated with the blockchain, data to be queried in encrypted data stored in the blockchain;
 - determining, through a smart contract, whether the one blockchain node has a permission to decrypt the data to be queried;
 - if the one blockchain node has the permission, sending the data to be queried to an encryption device through the smart contract to cause the encryption device to decrypt the data to be queried and return data obtained from the decryption to the one blockchain node; and
 - if the one blockchain node does not have the permission, refusing to send the data to be queried to the encryption device.

5. The method according to claim 4, wherein:
each encrypted data stored in the blockchain comprises an unencrypted part; and
the determining, by the one blockchain node associated with the blockchain, data to be queried in encrypted data stored in the blockchain comprises:
determining, by the one blockchain node, a data query condition;
determining, through the smart contract and according to the data query condition, whether the unencrypted part comprised in each encrypted data stored in the blockchain satisfies the data query condition;
if the data query condition is satisfied, using the encrypted data containing the unencrypted part that satisfies the data query condition as data to be queried; and
if the data query condition is not satisfied, not using any encrypted data as data to be queried.

6. The method according to claim 4, wherein, when the one blockchain node has a permission to decrypt the data to be queried, the method further comprises:
determining, through the smart contract, a second value corresponding to the data returned by the encryption device, the second value being used to represent a value deducted from an account of the one blockchain node; and
sending, through the smart contract, the one blockchain node's node identifier and the second value to other blockchain nodes associated with the blockchain to cause each of the other blockchain nodes to store the node identifier and the second value in the blockchain after performing consensus verification on the node identifier and the second value with success.

7. The method according to claim 4, wherein, when the one blockchain node has the permission to decrypt the data to be queried, the method further comprises:
determining, through the smart contract, a third value corresponding to the data and node identifiers of other blockchain nodes sharing the data, the third value being used to represent a value added into accounts of the other blockchain nodes sharing the data; and
sending, through the smart contract, the determined node identifiers and the third value to the other blockchain nodes to cause each of the other blockchain nodes to store the determined node identifiers and the third value in the blockchain after performing consensus verification on the determined node identifiers and the third value with success.

8. The method according to claim 4, further comprising:

sending, by the blockchain node, a refill request to a refill device to cause the refill device to determine a refill certificate according to the refill request and return the refill certificate to the blockchain node; the refill certificate comprising a fourth value and the fourth value being used to represent a value added into an account of the one blockchain node; and

sending the one blockchain node's node identifier and the refill certificate to other blockchain nodes associated with the blockchain to cause each of the other blockchain nodes to store the node identifier and the fourth value in the blockchain after performing consensus verification on the node identifier and the refill certificate with success.

9. A system implementable as a blockchain node associated with a blockchain, the system comprising a processor and a non-transitory computer-readable storage medium storing instructions that, when executed by the processor, cause the processor to perform a data storage method, the method comprising:

sending data to an encryption device to cause the encryption device to encrypt the data and return the encrypted data to the blockchain node;

receiving the encrypted data returned by the encryption device; and

sending the encrypted data to other blockchain nodes associated with the blockchain to cause each of the other blockchain nodes to store the encrypted data in the blockchain after performing consensus verification on the encrypted data with success.

10. The system according to claim 9, wherein the method further comprises:

determining a first value corresponding to the data through a smart contract, the first value being used to represent a value added into an account of the blockchain node; and

sending the blockchain node's own node identifier and the first value to the other blockchain nodes to cause the node identifier and the first value to be stored in the blockchain after a consensus verification on the node identifier and the first value by the blockchain nodes passed.

11. The system according to claim 9, wherein the encryption device is caused to encrypt a part of the data.

12. The system according to claim 9, wherein the method further comprises:

determining, by one of the blockchain nodes associated with the blockchain, data to be queried in encrypted data stored in the blockchain;

determining, through a smart contract, whether the one blockchain node has a permission to decrypt the data to be queried;

if the one blockchain node has the permission, sending the data to be queried to an encryption device through the smart contract to cause the encryption device to decrypt the data to be queried and return data obtained from the decryption to the one blockchain node; and

if the one blockchain node does not have the permission, refusing to send the data to be queried to the encryption device.

13. The system according to claim 12, wherein:

each encrypted data stored in the blockchain comprises an unencrypted part; and

the determining, by the one blockchain node, data to be queried in encrypted data stored in the blockchain comprises:

determining, by the one blockchain node, a data query condition;

determining, through the smart contract and according to the data query condition, whether the unencrypted part comprised in each encrypted data stored in the blockchain satisfies the data query condition;

if the data query condition is satisfied, using the encrypted data containing the unencrypted part that satisfies the data query condition as data to be queried; and

if the data query condition is not satisfied, not using any encrypted data as data to be queried.

14. The system according to claim 12, wherein, when the one blockchain node has a permission to decrypt the data to be queried, the method further comprises:

determining, through the smart contract, a second value corresponding to the data returned by the encryption device, the second value being used to represent a value deducted from an account of the one blockchain node; and

sending, through the smart contract, the one blockchain node's node identifier and the second value to other blockchain nodes to cause each of the other blockchain nodes to store

the node identifier and the second value in the blockchain after performing consensus verification on the node identifier and the second value with success.

15. The system according to claim 12, wherein, when the one blockchain node has the permission to decrypt the data to be queried, the method further comprises:

determining, through the smart contract, a third value corresponding to the data and node identifiers of other blockchain nodes sharing the data, the third value being used to represent a value added into accounts of the other blockchain nodes sharing the data; and

sending, through the smart contract, the determined node identifiers and the third value to the other blockchain nodes to cause each of the other blockchain nodes to store the determined node identifiers and the third value in the blockchain after performing consensus verification on the determined node identifiers and the third value with success.

16. The system according to claim 12, wherein the method further comprises:

sending, by the one blockchain node, a refill request to a refill device to cause the refill device to determine a refill certificate according to the refill request and return the refill certificate to the one blockchain node; the refill certificate comprising a fourth value and the fourth value being used to represent a value added into an account of the one blockchain node; and

sending the one blockchain node's node identifier and the refill certificate to other blockchain nodes to cause each of the other blockchain nodes to store the node identifier and the fourth value in the blockchain after performing consensus verification on the node identifier and the refill certificate with success.

17. A data query method, comprising:

determining, by a blockchain node associated with a blockchain, data to be queried in encrypted data stored in the blockchain;

determining, through a smart contract, whether the blockchain node has a permission to decrypt the data to be queried;

if the blockchain node has the permission, sending the data to be queried to an encryption device through the smart contract to cause the encryption device to decrypt the data to be queried and return data obtained from the decryption to the blockchain node; and

if the blockchain node does not have the permission, refusing to send the data to be

queried to the encryption device.

18. The method according to claim 17, wherein:

each encrypted data stored in the blockchain comprises an unencrypted part; and

the determining, by the blockchain node in the blockchain, data to be queried in encrypted data stored in a blockchain comprises:

determining, by the blockchain node, a data query condition;

determining, through the smart contract and according to the data query condition, whether the unencrypted part comprised in each encrypted data stored in the blockchain satisfies the data query condition;

if the data query condition is satisfied, using the encrypted data containing the unencrypted part that satisfies the data query condition as data to be queried; and

if the data query condition is not satisfied, not using any encrypted data as data to be queried.

19. The method according to claim 17, wherein, when the blockchain node has a permission to decrypt the data to be queried, the method further comprises:

determining, through the smart contract, a second value corresponding to the data returned by the encryption device, the second value being used to represent a value deducted from an account of the blockchain node; and

sending, through the smart contract, the blockchain node's node identifier and the second value to other blockchain nodes in the blockchain to cause each of the other blockchain nodes to store the node identifier and the second value in the blockchain after performing consensus verification on the node identifier and the second value with success.

20. The method according to claim 17, wherein, when the blockchain node has the permission to decrypt the data to be queried, the method further comprises:

determining, through the smart contract, a third value corresponding to the data and node identifiers of the other blockchain nodes sharing the data, the third value being used to represent a value added into accounts of the other blockchain nodes sharing the data; and

sending, through the smart contract, the determined node identifiers and the third value to the other blockchain nodes to cause each of the other blockchain nodes to store the determined node identifiers and the third value in the blockchain after performing consensus verification on the determined node identifiers and the third value with success.