Claims

1. A method, comprising:

receiving, from a first blockchain node of a blockchain network, a query for encrypted data stored in a blockchain, wherein the encrypted data comprises an unencrypted part;

determining, through one or more smart contracts and based on the unencrypted part, first attribute information of the encrypted data;

determining whether the first blockchain node has permission to query data associated with the first attribute information;

in response to determining that the first blockchain node has the permission:

sending the encrypted data to a device to decrypt the encrypted data to obtain decrypted data and return the decrypted data to the first blockchain node, wherein the device is a third-party device that is not a blockchain node;

after the decrypted data is returned to the first blockchain node, determining, through the one or more smart contracts, an expense to be deducted from an account of the first blockchain node for querying the encrypted data; and

sending a node identifier of the first blockchain node and the expense to other blockchain nodes of the blockchain network, enabling each of the other blockchain nodes to store the node identifier and the expense in the blockchain after the node identifier and the expense are successfully verified through at least a first consensus verification.

2. The method of claim 1, further comprising:

determining, through the one or more smart contracts, a second node identifier of a second blockchain node of the blockchain network sharing the encrypted data, and an award to be added into a second account of the second blockchain node for sharing the encrypted data; and

sending the second node identifier and the award to the other blockchain nodes, enabling each of the other blockchain nodes to store the second node identifier and the award in the blockchain after the second node identifier and the award are successfully verified through at least a second consensus verification.

3. The method of claim 1, further comprising:

sending, by the first blockchain node, a refill request to a refill device, enabling the refill device to determine a refill certificate according to the refill request and return the refill certificate to the first blockchain node, wherein the refill certificate contains a value that is added into the account of the first blockchain node; and

sending the node identifier and the refill certificate to the other blockchain nodes, enabling each of the other blockchain nodes to store the node identifier and the value in the blockchain after at least a second consensus verification on the node identifier and the refill certificate is successfully performed.

4. The method of claim 3, further comprising: sending the value to the other blockchain nodes, enabling each of the other blockchain nodes to compare the sent value and the value contained in the refill certificate during the at least second consensus verification.

5. The method of claim 1, further comprising:

sending, by a second blockchain node of the blockchain network, unencrypted data to the device, enabling the device to encrypt the unencrypted data and return the encrypted data to the second blockchain node;

determining, through the one or more smart contracts, an award to be added into a second account of the second blockchain node for sharing the encrypted data; and

sending the encrypted data, a second node identifier of the second blockchain node, and the award to the blockchain network to store the encrypted data, the second node identifier, and the award in the blockchain after the encrypted data, the second node identifier, and the award are successfully verified through at least a second consensus verification.

6. A system, comprising:

one or more processors; and

one or more non-transitory computer-readable storage medium storing instructions that, when executed by the one or more processors, cause the one or more processors to perform operations comprising:

receiving, from a first blockchain node of a blockchain network, a query for encrypted data stored in a blockchain, wherein the encrypted data comprises an unencrypted part;

determining, through one or more smart contracts and based on the unencrypted part, first attribute information of the encrypted data;

determining whether the first blockchain node has permission to query data associated with the first attribute information;

in response to determining that the first blockchain node has the permission:

sending the encrypted data to a device to decrypt the encrypted data to obtain decrypted data and return the decrypted data to the first blockchain node, wherein the device is a third-party device that is not a blockchain node;

after the decrypted data is returned to the first blockchain node, determining, through the one or more smart contracts, an expense to be deducted from an account of the first blockchain node for querying the encrypted data; and

sending a node identifier of the first blockchain node and the expense to other blockchain nodes of the blockchain network, enabling each of the other blockchain nodes to store the node identifier and the expense in the blockchain after the node identifier and the expense are successfully verified through at least a first consensus verification.

7. The system of claim 6, wherein the operations further comprise:

determining, through the one or more smart contracts, a second node identifier of a second blockchain node of the blockchain network sharing the encrypted data, and an award to be added into a second account of the second blockchain node for sharing the encrypted data; and

sending the second node identifier and the award to the other blockchain nodes, enabling each of the other blockchain nodes to store the second node identifier and the award in the blockchain after the second node identifier and the award are successfully verified through at least a second consensus verification.

8. The system of claim 6, wherein the operations further comprise:

sending, by the first blockchain node, a refill request to a refill device, enabling the refill device to determine a refill certificate according to the refill request and return the refill certificate to the first blockchain node, wherein the refill certificate contains a value that is added into the account of the first blockchain node; and

sending the node identifier and the refill certificate to the other blockchain nodes, enabling each of the other blockchain nodes to store the node identifier and the value in the blockchain after at least a second consensus verification on the node identifier and the refill certificate is successfully performed.

9. The system of claim 8, wherein the operations further comprise: sending the value to the other blockchain nodes, enabling each of the other blockchain nodes to compare the sent value and the value contained in the refill certificate during the at least second consensus verification.

10. The system of claim 6, wherein the operations further comprise:

sending, by a second blockchain node of the blockchain network, unencrypted data to the device, enabling the device to encrypt the unencrypted data and return the encrypted data to the second blockchain node;

determining, through the one or smart contracts, an award to be added into a second account of the second blockchain node for sharing the encrypted data; and

sending the encrypted data, a second node identifier of the second blockchain node, and the award to the blockchain network to store the encrypted data, the second node identifier, and the award in the blockchain after the encrypted data, the second node identifier, and the award are successfully verified through at least a second consensus verification.

11. A non-transitory computer-readable storage medium storing instructions that, when executed by a processor, cause the processor to perform operations comprising:

receiving, from a first blockchain node of a blockchain network, a query for encrypted data stored in a blockchain, wherein the encrypted data comprises an unencrypted part;

determining, through one or more smart contracts and based on the unencrypted part, first attribute information of the encrypted data;

determining whether the first blockchain node has permission to query data associated with the first attribute information;

in response to determining that the first blockchain node has the permission:

sending the encrypted data to a device to decrypt the encrypted data to obtain decrypted data and return the decrypted data to the first blockchain node, wherein the device is a third-party device that is not a blockchain node;

after the decrypted data is returned to the first blockchain node, determining, through the one or more smart contracts, an expense to be deducted from an account of the first blockchain node for querying the encrypted data; and

sending a node identifier of the first blockchain node and the expense to other blockchain nodes of the blockchain network, enabling each of the other blockchain nodes to store the node identifier and the expense in the blockchain after the node identifier and the expense are successfully verified through at least a first consensus verification.

12. The non-transitory computer-readable storage medium of claim 11, wherein the operations further comprise:

determining, through the one or more smart contracts, a second node identifier of a second blockchain node of the blockchain network sharing the encrypted data, and an award to be added into a second account of the second blockchain node for sharing the encrypted data; and

sending the second node identifier and the award to the other blockchain nodes, enabling each of the other blockchain nodes to store the second node identifier and the award in the blockchain after the second node identifier and the award are successfully verified through at least a second consensus verification.

13. The non-transitory computer-readable storage medium of claim 11, wherein the operations further comprise:

sending, by the first blockchain node, a refill request to a refill device, enabling the refill device to determine a refill certificate according to the refill request and return the refill certificate to the first blockchain node, wherein the refill certificate contains a value that is added into the account of the first blockchain node; and

sending the node identifier and the refill certificate to the other blockchain nodes, to cause enabling each of the other blockchain nodes to store the node identifier and the value in the blockchain after at least a second consensus verification on the node identifier and the refill certificate is successfully performed.

14. The non-transitory computer-readable storage medium of claim 13, wherein the operations further comprise: sending the value to the other blockchain nodes, enabling each of

the other blockchain nodes to compare the sent value and the value contained in the refill certificate during the at least second consensus verification.

15. The method of claim 1, wherein the first blockchain node has a permission to query preset data associated with second attribute information; and determining whether the first block chain node has permission to query data associated with the first attribute information comprises: determining whether the second attribute information comprises the first attribute information.

16. The system of claim 6, wherein the first blockchain node has a permission to query preset data associated with second attribute information; and determining whether the first block chain node has permission to query data associated with the first attribute information comprises: determining whether the second attribute information comprises the first attribute information.

17. The non-transitory computer-readable storage medium of claim 11, wherein the first blockchain node has a permission to query preset data associated with second attribute information; and determining whether the first block chain node has permission to query data associated with the first attribute information comprises: determining whether the second attribute information comprises the first attribute information.