

CLAIMS

What is claimed is:

1. A method for authorizing a blockchain data access, comprising:

obtaining, by a blockchain platform, a data access request from a third-party institution, wherein the data access request comprises a user ID of data access, a data scope, and a random number of a signature, wherein the random number of the signature is generated by the third-party institution by receiving the random number sent by the client terminal and by signing on the random number, and wherein the random number sent by the client terminal is generated after the client terminal receives an authorization request sent by the third-party institution and determines to authorize the blockchain data access from the third-party institution; the third-party institution is independent from the blockchain platform;

using, by the blockchain platform, a public key of the third-party institution sent by the client terminal to verify the random number of the signature; using, by the blockchain platform, a data scope of data access sent by the client terminal to verify the data scope comprised in the data access request; and

after determining that the verification is passed, sending, by the blockchain platform, data ciphertext corresponding to the user ID to the third-party institution, such that the third-party institution decrypts the data ciphertext using a data secret key sent by the client terminal.

2. The method according to claim 1, wherein, before sending data ciphertext corresponding to the user ID to the third-party institution, the method further comprises:

determining, by the blockchain platform, that a timer of the data access request has not timed out, wherein the timer of the data access request is started after receiving data verification

information sent from the client terminal.

3. The method according to claim 1 or 2, wherein, before obtaining the data access request from the third-party institution, the method further comprises:

obtaining, by the blockchain platform, data verification information sent by the client terminal, wherein the data verification information comprises the random number, the public key of the third-party institution, the data scope of data access, and a time of data access; and

starting, by the blockchain platform, a timer of the data access request according to the time of data access, and registering the random number, the public key of the third-party institution, and the data scope of data access.

4. The method according to claim 3, wherein, before obtaining the data verification information sent by the client terminal, the method further comprises:

obtaining, by the blockchain platform, data storage information sent by the client terminal, wherein the data storage information comprises the user ID and the data ciphertext corresponding to the user ID, and wherein the data ciphertext is obtained after encrypting data by the client terminal using a symmetric secret key of the client terminal; and

storing, by the blockchain platform, the data ciphertext corresponding to the user ID and the user ID.

5. The method according to claim 4, wherein, after storing the data ciphertext corresponding to the user ID and the user ID, the method further comprises:

obtaining, by the blockchain platform, a new data ciphertext sent by the client terminal,

wherein the new data ciphertext is obtained after encrypting a new data by the client terminal using the symmetric secret key; and

overwriting, by the blockchain platform, the data ciphertext with the new data ciphertext.

6. The method according to claim 4, wherein, after storing the data ciphertext corresponding to the user ID and the user ID, the method further comprises:

obtaining, by the blockchain platform, a data request sent by the client terminal;

sending, by the blockchain platform, the data ciphertext to the client terminal, such that the client terminal decrypts the data ciphertext and encrypts the data with a new symmetric secret key;

obtaining, by the blockchain platform, a data storage request sent by the client terminal, wherein the data storage request comprises a new data ciphertext that is encrypted by the client terminal using the new symmetric secret key; and

overwriting, by the blockchain platform, the data ciphertext with the new data ciphertext.

7. A blockchain data access authorization apparatus, comprising:

an obtaining unit configured to obtain a data access request from a third-party institution, wherein the data access request comprises a user ID of data access, a data scope, and a random number of a signature, wherein the random number of the signature is generated by the third-party institution by receiving the random number sent by the client terminal and by signing on the random number, and wherein the random number sent by the client terminal is generated after the client terminal receives an authorization request sent by the third-party institution and determines to authorize the blockchain data access from the third-party institution; the third-party

institution is independent from the blockchain platform;

a processing unit configured to use a public key of the third-party institution sent by the client terminal to verify the random number of the signature; and use a data scope of data access sent by the client terminal to verify the data scope comprised in the data access request; and

a sending unit configured to, after determining that the verification is passed, send data ciphertext corresponding to the user ID to the third-party institution, such that the third-party institution decrypts the data ciphertext using a data secret key sent by the client terminal.

8. The apparatus according to claim 7, wherein the processing unit is further configured to:

before sending the data ciphertext corresponding to the user ID to the third-party institution, determine that a timer of the data access request has not timed out, wherein the timer of the data access request is started after receiving data verification information sent from the client terminal.

9. The apparatus according to claim 7 or 8, wherein the processing unit is further configured to:

before obtaining the data access request from the third-party institution, obtain data verification information sent by the client terminal, wherein the data verification information comprises the random number, the public key of the third-party institution, the data scope of data access, and a time of data access; and

start a timer of the data access request according to the time of data access, and registering the random number, the public key of the third-party institution, and the data scope of data access.

10. The apparatus according to claim 9, wherein the processing unit is further configured to:
before obtaining the data verification information sent by the client terminal, obtain data storage information sent by the client terminal, wherein the data storage information comprises the user ID and the data ciphertext corresponding to the user ID, and wherein the data ciphertext is obtained after encrypting the data by the client terminal using a symmetric secret key of the client terminal; and
store the data ciphertext corresponding to the user ID and the user ID.

11. The apparatus according to claim 10, wherein the processing unit is further configured to:
after storing the data ciphertext corresponding to the user ID and the user ID, obtain a new data ciphertext sent by the client terminal, wherein the new data ciphertext is obtained after encrypting a new data by the client terminal using the symmetric secret key; and
overwrite the data ciphertext with the new data ciphertext.

12. The apparatus according to claim 10, wherein the processing unit is further configured to:
obtain a data request sent by the client terminal;
send the data ciphertext to the client terminal, such that the client terminal decrypts the data ciphertext and encrypts the data with a new symmetric secret key;
obtain a data storage request sent by the client terminal, wherein the data storage request includes a new data ciphertext that is encrypted by the client terminal using the new symmetric

secret key; and

overwrite the data ciphertext with the new data ciphertext.

13. A computing device, comprising:

a memory for storing program instructions; and

a processor configured to call the program instructions stored in the memory, and execute a method according to any of claims 1 to 6 according to the obtained program.

14. A computer-readable non-volatile storage medium, comprising computer-readable instructions for, when a computer reads and executes the computer-readable instructions, causing the computer to execute a method according to any claims 1 to 6.

15. A blockchain data access authorization device, comprising:

at least one processor; and

a memory communicatively coupled to the at least one processor; wherein,

the memory stores instructions executable by the at least one processor, and the instructions are executed by the at least one processor to enable the at least one processor to perform the execution of a method according to any of claims 1 to 6.