CLAIMS

What is claimed is:

1. A method for auditing data, the method comprising:

in response to receiving a query request, sending, by a proxy device, the query request to multiple service provider devices, wherein each service provider device determines an encrypted query result that corresponds to the query request based on the query request, and stores the encrypted query result as a result to be audited in a blockchain;

in response to receiving an audit request for the query request, obtaining, by the proxy device, the result to be audited that is stored by each service provider device from the blockchain, and sending the audit request to one of the multiple service provider devices, wherein the service provider device returns the encrypted query result that corresponds to the query request based on the audit request, and uses the encrypted query result as a standard result; and

auditing, by the proxy device, the service provider device based on the result to be audited and the standard result.

2. The method according to claim 1, wherein after receiving the query request, the method further comprises:

determining a serial number that corresponds to the query request; and

sending the serial number to each of the multiple service provider devices, wherein each service provider device establishes and stores a mapping relationship between the serial number and the encrypted query result determined by the service provider device.

3. The method according to claim 2, wherein after sending the query request to multiple service provider devices, the method further comprises , for each lender device:

receiving a storage address that corresponds to the result to be audited in the blockchain and that is returned by the service provider device; and

establishing and storing a mapping relationship between the service provider device, the storage address, and the serial number.

4. The method according to claim 3, wherein the audit request comprises the serial number that corresponds to the query request; and

obtaining the result to be audited that is stored by each service provider device from the blockchain comprises:

obtaining the result to be audited that corresponds to the serial number and that is stored by the service provider device in the blockchain based on a locally stored mapping relationship between each service provider device, each serial number, and each storage address.

5. The method according to claim 1, wherein the query request is a loan query request; and

after sending the query request to multiple service provider devices, the method further comprises:

receiving the result to be audited that is returned by each service provider device; and

processing each result to be audited to obtain and return a total amount of loans.

6. A method for auditing data, the method comprising:

determining, by a service provider device when receiving a query request sent by a proxy device, an encrypted query result that corresponds to the query request based on the query request, and storing, by the service provide device, the encrypted query result as a result to be audited in a blockchain;

determining, by the service provider device, the encrypted query result that corresponds to the query request based on an audit request when receiving the audit request sent by the proxy device for the query request, and using the encrypted query result as a standard result; and

returning, from the service provider device, the standard result to the proxy device, wherein the proxy device audits the service provider device based on the standard result and the result to be audited that is obtained from the blockchain.

7. The method according to claim 6, wherein determining an encrypted query result that corresponds to the query request based on the query request, and storing the encrypted query result as a result to be audited in a blockchain comprises:

generating, by the service provider device, a random number, and determining a query

result based on the query request; and

combining the random number and the query result, performing irreversible encryption on a result obtained through combination, and storing an obtained encrypted result as the result to be audited in the blockchain.

8. The method according to claim 7, wherein after determining an encrypted query result that corresponds to the query request, and storing the encrypted query result as a result to be audited in a blockchain, the method further comprises:

determining, by the service provider device, a serial number that corresponds to the query request; and

establishing and storing a mapping relationship between the query result, the random number, and the serial number.

9. The method according to claim 8, wherein after determining an encrypted query result that corresponds to the query request, and storing the encrypted query result as a result to be audited in a blockchain, the method further comprises:

returning a storage address of the result to be audited and the serial number to the proxy device, so that the proxy device establishes and stores a mapping relationship between the storage address and the serial number.

10. The method according to claim 7, wherein , performing irreversible encryption on a result obtained through combination comprises performing at least one of a message digest algorithm 5 (MD5), a hash algorithm, and a secure hash standard (SHS).

11. The method according to claim 8, wherein the audit request comprises the serial number that corresponds to the query request; and

determining the encrypted query result that corresponds to the query request, and using the encrypted query result as a standard result comprises:

determining a random number and a query result that correspond to the serial number comprised in the audit request based on a locally stored mapping relationship between

each query result, each random number, and each serial number; and

combining the determined random number and the query result, performing irreversible encryption on a result obtained through combination, and using an obtained encrypted result as the standard result.

12. The method according to claim 6, wherein the query request is a loan query request; and

determining an encrypted query result that corresponds to the query request based on the query request, and storing the encrypted query result as a result to be audited in a blockchain comprises:

generating, by the service provider device, a random number, and determining an amount of loans based on the query request; and

combining the random number and the amount of loans, performing irreversible encryption on a result obtained through combination, and storing an obtained encrypted result as the result to be audited in the blockchain.

13. A device for auditing data, the device comprising multiple modules configured to perform the method of any one of claims 1 to 5.

14. A device for auditing data, comprising multiple modules configured to perform the method of any one of claims 6 to 12.

15. A proxy device, comprising one or more processors and a memory, wherein the memory stores a program, and the program is configured to be used by the one or more processors to perform the steps of any one of claims 1 to 5.

16. A service provider device, comprising one or more processors and a memory, wherein the memory stores a program, and the program is configured to be used by the one or more processors to perform the steps of any one of claims 6 to 12.

17. A method for auditing data, the method comprising:

in response to receiving a query request, sending, by a proxy device, the query request to multiple service provider devices;

determining, by each of the multiple service provider devices, an encrypted query result that corresponds to the query request based on the query request;

storing, by each of the multiple service provide devices, the encrypted query result as a result to be audited in a blockchain;

in response to receiving an audit request for the query request, obtaining, by the proxy device, the result to be audited that is stored by each of the multiple service provider devices from the blockchain;

sending the audit request to one of the multiple service provider devices;

determining, by the service provider device, the encrypted query result that corresponds to the query request based on an audit request, and using the encrypted query result as a standard result; and

returning, from the service provider device, the standard result to the proxy device; and

auditing, by the proxy device, the service provider device based on the result to be audited and the standard result.

18. The method according to claim 17, wherein the method further comprises:

determining, by the proxy device, a serial number that corresponds to the query request; and

sending, by the proxy device, the serial number to each of the multiple service provider devices.

19. The method according to claim 18, wherein after sending the query request to multiple service provider devices, the method further comprises, for each of the multiple service provider devices:

receiving, by the proxy device, a storage address that corresponds to the result to be audited in the blockchain and that is returned by the service provider device; and

establishing and storing, by the proxy device, a mapping relationship between the service provider device, the storage address, and the serial number.

20. The method according to claim 19, wherein the audit request comprises the serial number that corresponds to the query request; and

obtaining the result to be audited that is stored by each service provider device from the blockchain comprises:

obtaining the result to be audited that corresponds to the serial number and that is stored by the multiple service provider devices in the blockchain based on a locally stored mapping relationship between each service provider device, each serial number, and each storage address.

21. The method according to claim 17, wherein the query request is a loan query request, and the method further comprises:

receiving, at the proxy device, the result to be audited that is returned by each service provider device; and

processing, by the proxy device, each result to be audited to obtain and return a total amount of loans.

22. The method according to claim 6, wherein determining an encrypted query result that corresponds to the query request based on the query request, and storing the encrypted query result as a result to be audited in a blockchain comprises, for each of the multiple service provider devices:

generating, by the service provider device, a random number, and determining a query result based on the query request; and

combining the random number and the query result, performing irreversible encryption on a result obtained through combination, and storing an obtained encrypted result as the result to be audited in the blockchain.

23. The method according to claim 22, wherein the method further comprises, for each of the multiple service provider devices:

determining, by the service provider device, a serial number that corresponds to the query

request; and

establishing and storing a mapping relationship between the query result, the random number, and the serial number.

24. The method according to claim 23, wherein the method further comprises, for each of the multiple service provider devices:

returning a storage address of the result to be audited and the serial number to the proxy device, so that the proxy device establishes and stores a mapping relationship between the storage address and the serial number.

25. The method according to claim 22, wherein, performing irreversible encryption on a result obtained through combination comprises performing at least one of a message digest algorithm 5 (MD5), a hash algorithm, and a secure hash standard (SHS).

26. The method according to claim 23, wherein the audit request comprises the serial number that corresponds to the query request; and

determining the encrypted query result that corresponds to the query request, and using the encrypted query result as a standard result comprises:

determining a random number and a query result that correspond to the serial number comprised in the audit request based on a locally stored mapping relationship between each query result, each random number, and each serial number; and

combining the determined random number and the query result, performing irreversible encryption on a result obtained through combination, and using an obtained encrypted result as the standard result.

27. The method according to claim 17, wherein the query request is a loan query request; and

determining an encrypted query result that corresponds to the query request based on the query request, and storing the encrypted query result as a result to be audited in a blockchain comprises:

generating, by the service provider device, a random number, and determining an

amount of loans based on the query request; and

combining the random number and the amount of loans, performing irreversible encryption on a result obtained through combination, and storing an obtained encrypted result as the result to be audited in the blockchain.

28. A device, comprising one or more processors and a memory, wherein the memory stores a program, and the program is configured to be used by the one or more processors to perform the steps of any one of claims 17 to 27.

29. A device, comprising multiple modules configured to perform the steps of any one of claims 17 to 27.