CLAIMS

1. A computer-implemented method, comprising:

receiving, by a particular service provider server and from a proxy server, a query request;

in response to receiving the query request, generating, by the particular service provider server, a first encrypted query result, wherein the first encrypted query result is generated based on an irreversible encryption algorithm, wherein the query request comprises a loan query request, and generating, by the particular service provider server, the first encrypted query result comprises:

generating, by the particular service provider server, a random number;

determining, by the particular service provider server, an amount of loans based on the query request;

combining the random number and the amount of loans to render a combined result; and

encrypting the combined result based on the irreversible encryption algorithm to generate the first encrypted query result;

storing, by the particular service provider server, the first encrypted query result in a blockchain that is associated with the particular service provider server;

receiving, by the particular service provider server, an audit request from the proxy server;

generating, by the particular service provider server, a second encrypted query result, wherein the second encrypted query result is generated based on the same irreversible encryption algorithm; and

transmitting, by the particular service provider server, the second encrypted query result to the proxy server, for use by the proxy server in generating a response to the audit request based at least on comparing the second encrypted query result with the first encrypted query result.

2. The method of claim 1, wherein generating the first encrypted query result comprises:

determining, by the particular service provider server, a query result based on the query request;

generating the random number;

combining the random number and the query result to render the combined result; and

encrypting the combined result based on the irreversible encryption algorithm to generate the first encrypted query result.

3. The method of claim 2, wherein after storing the first encrypted query result in the blockchain, the method further comprises:

determining, by the particular service provider server, a serial number that is associated with the query request; and

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

4. The method of claim 3, wherein after storing the first encrypted query result in the blockchain, the method further comprises:

sending, to the proxy server by the particular service provider server, a storage address of the first encrypted query result and the serial number, wherein the proxy server establishes and stores a mapping relationship between the storage address and the serial number.

5. The method of claim 1, wherein the irreversible encryption algorithm comprises at least one of a message digest algorithm 5 (MD5), a hash algorithm, and a secure hash standard (SHS).

6. The method of claim 1, wherein the query request specifies a service to collectively be performed by the particular service provider server and a plurality of other service provider servers.

7. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

receiving, by a particular service provider server and from a proxy server, a query request;

in response to receiving the query request, generating, by the particular service provider server, a first encrypted query result, wherein the first encrypted query result is generated based on an irreversible encryption algorithm, wherein the query request comprises a loan query request, and generating, by the particular service provider server, the first encrypted query result comprises:

generating, by the particular service provider server, a random number;

determining, by the particular service provider server, an amount of loans based on the query request;

combining the random number and the amount of loans to render a combined result; and

encrypting the combined result based on the irreversible encryption algorithm to generate the first encrypted query result;

storing, by the particular service provider server, the first encrypted query result in a blockchain that is associated with the particular service provider server;

receiving, by the particular service provider server, an audit request from the proxy server;

generating, by the particular service provider server, a second encrypted query result, wherein the second encrypted query result is generated based on the same irreversible encryption algorithm; and

transmitting, by the particular service provider server, the second encrypted query result to the proxy server, for use by the proxy server in generating a response to the audit request based at least on comparing the second encrypted query result with the first encrypted query result.

8. The medium of claim 7, wherein generating the first encrypted query result comprises:

determining, by the particular service provider server, a query result based on the query request;

generating the random number;

combining the random number and the query result to render the combined result; and

encrypting the combined result based on the irreversible encryption algorithm to generate the first encrypted query result.

9. The medium of claim 8, wherein after storing the first encrypted query result in the blockchain, the operations further comprise:

determining, by the particular service provider server, a serial number that is associated with the query request; and

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

10. The medium of claim 9, wherein after storing the first encrypted query result in the blockchain, the operations further comprise:

sending, to the proxy server by the particular service provider server, a storage address of the first encrypted query result and the serial number, wherein the proxy server establishes and stores a mapping relationship between the storage address and the serial number.

11. The medium of claim 7, wherein the irreversible encryption algorithm comprises at least one of a message digest algorithm 5 (MD5), a hash algorithm, and a secure hash standard (SHS).

12. The medium of claim 7, wherein the query request specifies a service to collectively be performed by the particular service provider server and a plurality of other service provider servers.

13. A system comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform operations comprising:

receiving, by a particular service provider server and from a proxy server, a query request;

in response to receiving the query request, generating, by the particular service provider server, a first encrypted query result, wherein the first encrypted query result is generated based on an irreversible encryption algorithm, wherein the query request comprises a

loan query request, and generating, by the particular service provider server, the first encrypted query result comprises:

generating, by the particular service provider server, a random number;

determining, by the particular service provider server, an amount of loans based on the query request;

combining the random number and the amount of loans to render a combined result; and

encrypting the combined result based on the irreversible encryption algorithm to generate the first encrypted query result;

storing, by the particular service provider server, the first encrypted query result in a blockchain that is associated with the particular service provider server;

receiving, by the particular service provider server, an audit request from the proxy server;

generating, by the particular service provider server, a second encrypted query result, wherein the second encrypted query result is generated based on the same irreversible encryption algorithm; and

transmitting, by the particular service provider server, the second encrypted query result to the proxy server, for use by the proxy server in generating a response to the audit request based at least on comparing the second encrypted query result with the first encrypted query result.

14. The system of claim 13, wherein generating the first encrypted query result comprises:

determining, by the particular service provider server, a query result based on the query request;

generating the random number;

combining the random number and the query result to render the combined result; and

encrypting the combined result based on the irreversible encryption algorithm to generate the first encrypted query result.

15. The system of claim 14, wherein after storing the first encrypted query result in the blockchain, the operations further comprise:

determining, by the particular service provider server, a serial number that is associated with the query request; and

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

16. The system of claim 15, wherein after storing the first encrypted query result in the blockchain, the operations further comprise:

sending, to the proxy server by the particular service provider server, a storage address of the first encrypted query result and the serial number, wherein the proxy server establishes and stores a mapping relationship between the storage address and the serial number.

17. The system of claim 13, wherein the irreversible encryption algorithm comprises at least one of a message digest algorithm 5 (MD5), a hash algorithm, and a secure hash standard (SHS).