

CLAIMS

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

receiving a search request to obtain encrypted data associated with a user, the encrypted data being stored by a plurality of computing nodes of a blockchain network;

5 receiving, from the plurality of computing nodes of the blockchain network, the encrypted data associated with the user;

processing the encrypted data of each of the plurality of computing nodes of the blockchain network using a secure multi-party algorithm based on transfer of original data associated with the user to determine a search result comprising a serial number, wherein the
10 secure multi-party algorithm is configured to reveal a numerical value corresponding to the original data without revealing privacy data of any of the plurality of computing nodes of the blockchain network;

receiving an auditing request with respect to the search result, wherein the auditing request comprises an identity information;

15 for each computing node of the plurality of computing nodes, obtaining a key used by a respective computing node when generating the encrypted data to obtain the search result, and obtaining, as obtained to-be-audited data, to-be-audited data stored by the respective computing node in a trusted storage space, wherein the to-be-audited data stored by the respective computing node in the trusted storage space comprises: the encrypted data received
20 by the respective computing node from other computing nodes or generated by the respective computing node, and an identifier of the respective computing node corresponding to the encrypted data, wherein the identifier of the respective computing node corresponding to the encrypted data is the identifier of a source computing node that generated the encrypted data;

25 for each computing node of the plurality of computing nodes, determining, based on the identifier of the source computing node, the encrypted data generated by the source computing node from the obtained to-be-audited data;

for each computing node of the plurality of computing nodes, decrypting, based on the key of the respective computing node, the encrypted data in the to-be-audited data to obtain, as obtained original data, the original data of the respective computing node; and

30 auditing each computing node based on the obtained original data.

2. The method according to claim 1, wherein for each computing node, the encrypted data generated by the respective computing node is obtained by encrypting the original data determined to obtain the search result;

the original data is determined, after a search request to obtain the search result is received, by the respective computing node based on the search request; and

the encrypted data generated by the source computing node is sent to the other computing nodes for secure multi-party computation.

3. The method according to claim 1, wherein before obtaining the to-be-audited data stored by the respective computing node in the trusted storage space, the method further comprises:

receiving a storage address corresponding to the serial number of the search result returned by the respective computing node; and

establishing and storing a corresponding relationship between the storage address and the serial number.

4. The method according to claim 3, wherein the auditing request comprises the serial number of the search result.

5. The method according to claim 4, wherein obtaining the to-be-audited data stored by the respective computing node in the trusted storage space, comprises:

determining, as a determined storage address, the storage address corresponding to the serial number carried in the auditing request according to the corresponding relationship between stored serial numbers and storage addresses; and

obtaining the to-be-audited data from the trusted storage space according to the determined storage address.

6. The method according to claim 1, wherein the trusted storage space at least comprising: a blockchain.

7. An agent device, comprising one or more processors and memories storing a program, wherein the one or more processors are configured to perform a method according to any of claims 1 to 6.