

CLAIMS

What is claimed is:

1. A data sharing system, comprising:

members, wherein each member respectively is configured to maintain sharable private data, and to generate corresponding ciphertext index information for the shareable private data, the corresponding ciphertext index information comprising a ciphertext index of the shareable private data and information about a member that provides the shareable private data; and

a sharing platform, wherein the sharing platform is connected to each member and being configured to record ciphertext index information generated by each member in an index blockchain for sharing among all members; the sharing platform configured to forward a data acquisition request initiated by a data requester member to a data provider member; the data acquisition request comprising a ciphertext index of target data, and the sharing platform further configured to forward the target data corresponding to the data acquisition request returned by the data provider member to the data requester member, wherein the target data is encrypted by an identity public key of the data requester member,

characterised in that

the index blockchain is configured to receive a transaction of a complaint type for the target data, wherein the transaction comprises a complaint reason and related data, and wherein the transaction invokes a smart contract for processing the complaint,

and wherein the smart contract is used to verify the complaint reason based on the related data, and when the complaint reason is verified to be legitimate, an index information set corresponding to the target data shared in the index blockchain is added with an invalid identifier in the index blockchain, the index information set comprising a ciphertext index of the target data and member information of the data provider member.

2. The data sharing system according to claim 1, wherein the sharing platform is configured as a blockchain node of the index blockchain; and the sharing platform is configured to obtain ciphertext index information generated by each member, and configured to publish the ciphertext index information to the index blockchain; wherein

the sharing platform is configured to query, based on an information query request initiated by any member, corresponding ciphertext index information in an index blockchain ledger maintained by the sharing platform, and to return the ciphertext index information to the any member; and/or at least one member is configured to download the index blockchain ledger

maintained by the sharing platform to query ciphertext index information.

3. The data sharing system according to claim 1, wherein the sharing platform and each member are configured as blockchain nodes of the index blockchain, respectively; and each member being configured to separately publish generated ciphertext index information to the index blockchain, and to query ciphertext index information by using an index blockchain ledger maintained by the member; and/or wherein the sharing platform is configured as a blockchain node of a transaction blockchain; and the sharing platform further being configured to record a data sharing event between the data requester member and the data provider member into the transaction blockchain.

4. A data sharing method applied to a data requester member, the method comprising:
determining (102) an index information set corresponding to target data and recorded in an index blockchain, wherein the index information set comprises a ciphertext index of the target data and member information of a data provider of the target data, and the index information set is shared by the data provider to the index blockchain;

initiating (104) a data acquisition request to the data provider by using a sharing platform, wherein the data acquisition request comprises the ciphertext index of the target data;

receiving (106) response data returned by the sharing platform, wherein the response data corresponds to the data acquisition request and is encrypted by an identity public key of the data requester member;

characterised by

submitting a transaction of a complaint type for the response data to the index blockchain to invoke a smart contract for processing a complaint, wherein the transaction comprises a complaint reason and related data; and

the smart contract is used to verify the complaint reason based on the related data, and when the complaint reason is verified to be legitimate, the index information set is added with an invalid identifier in the index blockchain.

5. The method according to claim 4, wherein the sharing platform is configured as a node of the index blockchain; and the determining an index information set corresponding to target data and recorded in an index blockchain comprises:

generating a corresponding ciphertext index based on specific information of known target data; and

initiating a query request to the sharing platform, wherein the query request comprises the ciphertext index to instruct the sharing platform to query, from the index blockchain, an index information set comprising the ciphertext index; or downloading ledger data of the index

blockchain maintained by the sharing platform, so as to query the index information set that comprises the ciphertext index.

6. The method according to claim 4, wherein the data requester member is configured as a node of the index blockchain; and the determining an index information set corresponding to target data and recorded in an index blockchain comprises:

generating a corresponding ciphertext index based on specific information of known target data; and

querying, based on ledger data of the index blockchain maintained by the data requester member, an index information set that comprises the ciphertext index.

7. The method according to claim 4, wherein the data acquisition request further comprises the identity public key of the data requester member and a signature of the data requester member generated by using an identity private key of the data requester member, to facilitate verification by the data provider; and/ or

wherein the response data further comprises a signature of the data provider generated by using an identity private key of the data provider, to facilitate verification by the data requester member.

8. The method according to claim 4, wherein the index information set comprises a hash value of the target data; and the method further comprises:

performing hash computation on decrypted data corresponding to the response data; and

when a computed hash value is consistent with the hash value in the index information set, determining that the decrypted data is the target data.

9. The method according to claim 4, further comprising:

initiating a complaint request for the target data to the sharing platform, wherein the complaint request comprises a complaint reason and related data; wherein

when the complaint reason is verified to be legitimate based on the related data by the sharing platform or a smart contract invoked by the sharing platform from the index blockchain, the index information set is added with an invalid identifier in the index blockchain.

10. The method according to claim 4, further comprising:

publishing a data sharing event between the data requester member and the data provider to a transaction blockchain, wherein the data requester member is configured as a node of the transaction blockchain; or

sending the data sharing event to the sharing platform, so the sharing platform publishes the data sharing event to the transaction blockchain, wherein the sharing platform is configured

as a node of the transaction blockchain.

11. A data sharing method applied to a sharing platform, the method comprising:

publishing (302) an index information set corresponding to target data to an index blockchain, wherein the index information set comprises a ciphertext index of the target data and member information of a data provider of the target data, and the index information set is submitted by the data provider to the sharing platform;

forwarding (304) a data acquisition request initiated by a data requester to the data provider, wherein the data acquisition request comprises the ciphertext index of the target data;

returning (306) response data corresponding to the data acquisition request provided by the data provider to the data requester, wherein the response data is encrypted by an identity public key of the data requester; and

characterised by

receiving a transaction of a complaint type for the response data, wherein the transaction comprises a complaint reason and related data, and wherein the transaction invokes a smart contract for processing the complaint,

wherein the smart contract is used to verify the complaint reason based on the related data, and when the complaint reason is verified to be legitimate, the index information set is added with an invalid identifier in the index blockchain.

12. The method according to claim 11, further comprising:

receiving a query request initiated by the data requester, wherein the query request comprises a ciphertext index generated based on specific information of known target data; and querying an index information set comprising the ciphertext index from the index blockchain to inform the data requester.

13. The method according to claim 11, further comprising:

receiving a complaint request for the target data initiated by the data requester to the sharing platform, wherein the complaint request comprises a complaint reason and related data; and

when the complaint reason is verified to be legitimate based on the related data, adding an invalid identifier to the index information set in the index blockchain; and/ or

further comprising:

determining a data sharing event between the data requester and the data provider; and publishing the data sharing event to a transaction blockchain, wherein the sharing platform is configured as a node of the transaction blockchain.

14. An electronic device, comprising:

a processor; and
a memory, configured to store instructions executable by the processor; wherein
the processor runs the executable instructions to implement the method according to
any one of claims 4 to 13.