

CLAIMS

1. A computer-implemented data storage method, comprising:
 - receiving, by a data storage device, a data storage instruction including data to be stored and an identifier of the data;
 - 5 identifying a blockchain corresponding to the identifier, the blockchain being stored on blockchain network storage nodes of a data access system, wherein the blockchain is a first blockchain, and wherein the computer-implemented data storage method further comprises:
 - receiving, by a data query device, a data query instruction including a data identifier;
 - identifying a second blockchain that corresponds to the data identifier, the second blockchain
 - 10 being stored in the blockchain network storage nodes;
 - retrieving, from a node of the blockchain network storage nodes, the second blockchain;
 - decrypting data of the second blockchain based on a private key associated with the data identifier; and
 - querying, by the data query device, the data;
 - 15 identifying a key pair corresponding to the identifier, the key pair comprising a private key and a public key;
 - encrypting the data based on the public key to provide encrypted data;
 - updating the blockchain by storing the encrypted data in the blockchain wherein updating the first blockchain comprises:
 - 20 retrieving, from the particular blockchain network storage node, an encrypted data packet stored in the first blockchain;
 - decrypting the encrypted data packet by using the private key in the key pair to obtain all data that corresponds to the identifier in the encrypted data packet;
 - updating data that corresponds to the identifier in the encrypted data packet based on the data
 - 25 to be stored, to obtain updated data;
 - encrypting the updated data as an updated encrypted data packet by using the public key in the key pair;
 - adding a time stamp to the updated encrypted data packet; and
 - storing the updated encrypted data packet and the time stamp in the first blockchain; and
 - 30 storing the first blockchain in a particular blockchain network storage node of the blockchain network storage nodes, the particular blockchain network storage node associated with a data storage device.
2. The computer-implemented data storage method of claim 1, wherein the encrypted data is stored in a most-recently created block of the blockchain.
- 35 3. The computer-implemented data storage method of claim 1, wherein the data storage device is different from the blockchain network storage nodes and communicates with only the particular blockchain network storage node from among the blockchain network storage nodes for storing data.

4. The computer-implemented data storage method of claim 1, further comprising broadcasting, by the particular blockchain network storage node, the blockchain to other blockchain network storage nodes of the data access system.
5. The computer-implemented data storage method of claim 1, wherein the blockchain is identified by searching a stored data that contains mapping relationship between one or more identifiers and one or more blockchains.
6. The computer-implemented data storage method of claim 5, further comprising in response to determining that no blockchain is mapped to the identifier, generating the blockchain; and associating the blockchain to the identifier and a key pair associated with the identifier.
7. The computer-implemented data storage method of claim 6, further comprising: generating initial data based on the identifier; updating the initial data based on the data to be stored; generating the key pair that corresponds to the identifier; encrypting the initial data as an encrypted data packet that corresponds to the identifier by using the public key in the key pair; storing the encrypted data packet in the blockchain; and storing the blockchain in the particular blockchain network storage node.
8. The computer-implemented data storage method of claim 7, further comprising sending the key pair that corresponds to the identifier to one or more predetermined devices that store one or more key pairs.
9. The computer-implemented data storage method of claim 1, wherein the key pair is identified by searching stored data that contains a mapping relationship between one or more identifiers and one or more key pairs.
10. The computer-implemented data storage method of claim 1, further comprising: sending, by the data query device, a private key acquisition request to a computing device that stores a mapping relationship between one or more data identifiers and one or more key pairs, the private key acquisition request including the data identifier; and receiving the private key associated with the data identifier.
11. The computer-implemented data storage method of claim 1, wherein decrypting data of the second blockchain comprises: determining a most recently stored encrypted data packet in the blockchain based on a time sequence of storing encrypted data packets; and decrypting only the most recently stored encrypted data packet.
12. A computer-implemented data access system, comprising: one or more blockchain network storage nodes, nodes of the one or more blockchain network storage nodes storing one or more blockchains of data, each blockchain being associated to a respective identifier; and one or more data storage devices, each data storage device being configured to:

receive a data storage instruction that comprises data to be stored and an identifier,

determine a first blockchain and a first key pair associated with the identifier,

encrypt data based on a public key in the first key pair, and

5 store the encrypted data in network storage nodes of the first blockchain to update the first blockchain, each data storage device storing the encrypted data in a respective blockchain network storage node associated with a storage device wherein the storing comprises:

retrieving, from the respective blockchain network storage node, an encrypted data packet stored in the first blockchain;

10 decrypting the encrypted data packet by using a private key in the first key pair to obtain all data that corresponds to the identifier in the encrypted data packet;

updating data that corresponds to the identifier in the encrypted data packet based on the data to be stored, to obtain updated data;

15 encrypting the updated data as an updated encrypted data packet by using the public key in the first key pair;

adding a time stamp to the updated encrypted data packet; and

storing the updated encrypted data packet and the time stamp in the first blockchain; and one or more query devices, each query device configured to:

20 receive a data query instruction that comprises a data identifier,

determine a second blockchain and a second key pair that corresponds to the data identifier,

retrieve data of the second blockchain from the one or more blockchain network storage nodes,

25 decrypt the data based on a public key of the second key pair, and

query the data.

13. The computer-implemented data access system of claim 12, wherein at least one of the data storage devices is configured to:

30 in response to determining that no blockchain associated with the identifier is stored in the blockchain network storage nodes, generate the first blockchain and associated the identifier with the first blockchain.

14. The computer-implemented data access system of claim 12, wherein at least one of the query devices is configured to:

receive, from a blockchain network storage node, each encrypted data packet that corresponds to the data identifier in the second blockchain; and

35 determine a most recently stored encrypted data packet in the second blockchain based on a time sequence of storing encrypted data packets in the second blockchain, wherein the at least one of the query devices decrypts only the most recently stored encrypted data packet.

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

receiving a data storage instruction including data to be stored and an identifier of the data;

identifying a blockchain corresponding to the identifier, the blockchain stored on blockchain network storage nodes of a data access system, wherein the blockchain is a first blockchain, and the operations further comprise:

receiving, by a data query device, a data query instruction including a data identifier;

identifying a second blockchain that corresponds to the data identifier, the second blockchain stored in the blockchain network storage nodes;

retrieving, from a node of the blockchain network storage nodes, the second blockchain;

decrypting data of the second blockchain based on a private key associated with the data identifier; and

querying, by the data query device, the data;

identifying a key pair corresponding to the identifier, the key pair comprising a private key and a public key;

encrypting the data based on the public key to provide encrypted data;

updating the first blockchain by storing the encrypted data in the first blockchain, wherein updating the first blockchain comprises:

retrieving, from the blockchain network storage node, an encrypted data packet stored in the first blockchain;

decrypting the encrypted data packet by using the private key in the key pair to obtain all data that corresponds to the identifier in the encrypted data packet;

updating data that corresponds to the identifier in the encrypted data packet based on the data to be stored, to obtain updated data;

encrypting the updated data as an updated encrypted data packet by using the public key in the key pair;

adding a time stamp to the updated encrypted data packet; and

storing the updated encrypted data packet and the time stamp in the first blockchain; and

storing the first blockchain in a blockchain network storage node of the blockchain network storage nodes, the blockchain network storage node associated with a data storage device.

16. The non-transitory computer-readable medium of claim 15, wherein the blockchain is a first blockchain, and the operations further comprise:

receiving, by a data query device, a data query instruction including a data identifier;

identifying a second blockchain that corresponds to the data identifier, the second blockchain stored in the blockchain network storage nodes;

retrieving, from a node of the blockchain network storage nodes, the second blockchain;

decrypting data of the second blockchain based on a private key associated with the data identifier; and

querying, by the data query device, the data.

17. The non-transitory computer-readable medium of claim 15, wherein the blockchain is identified by searching a stored data that contains mapping relationship between one or more identifiers and one or more blockchains, and the operations further comprise:

5 in response to determining that no blockchain is mapped to the identifier, generating the blockchain, and associating the blockchain to the identifier and a key pair associated with the identifier.