

CLAIMS

1. A computer-implemented method, comprising:

obtaining, by a node device of a key receiver, a first derived key that is distributed by a node device of a key distributor, wherein the first derived key is derived from a derived key of the key distributor based on a service data permission type of the key receiver, wherein both the derived key of the key distributor and the first derived key are asymmetric encryption key pairs, and the first derived key comprises a first derived public key and a first derived private key, wherein obtaining the first derived key comprises obtaining, by the node device of the key receiver, the first derived public key and the first derived private key encrypted by a user public key of the key receiver from a distributed database of a blockchain;

encrypting service data based on the first derived key to obtain encrypted service data, comprising:

encrypting the service data by using the first derived public key to obtain first encrypted service data, wherein the encrypted service data comprises the first encrypted service data;

encrypting the service data by using an encryption key to obtain second encrypted service data; and

encrypting a decryption key corresponding to the encryption key by using the first derived key to obtain encrypted key data, wherein the encrypted service data comprises the second encrypted service data and the encrypted key data; and

sending the encrypted service data to the blockchain, so that the encrypted service data is recorded in the distributed database of the blockchain after the blockchain performs consensus verification on the encrypted service data.

2. The computer-implemented method of claim 1, further comprising:

sending a request transaction for the first derived private key to the blockchain, wherein the request transaction is encrypted by the user private key of the key receiver, so that the node device of the key distributor sends the first derived private key encrypted by the user public key of the key receiver to the blockchain after successfully verifying the request transaction based on the user public key of the key receiver.

3. The computer-implemented method of claim 1, wherein the first derived key is a key derived from the derived key of the key distributor through key derivation function (KDF) calculation based on a service data access permission type of the key receiver.
- 5 4. The method of claim 1, further comprising:
storing the first derived key and an identifier of the service data permission type in a local database of the key receiver.
- 10 5. The method of claim 4, wherein the sending the encrypted service data to the blockchain comprises:
sending the encrypted service data and the identifier of the service data permission type to the blockchain.
- 15 6. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:
obtaining, by a node device of a key receiver, a first derived key that is distributed by a node device of a key distributor, wherein the first derived key is derived from a derived key of the key distributor based on a service data permission type of the key receiver, wherein both the derived key of the key distributor and the first derived key are asymmetric encryption key
20 pairs, and the first derived key comprises a first derived public key and a first derived private key, wherein obtaining the first derived key comprises obtaining, by the node device of the key receiver, the first derived public key and the first derived private key encrypted by a user public key of the key receiver from a distributed database of a blockchain;
encrypting service data based on the first derived key to obtain encrypted service data,
25 comprising:
encrypting the service data by using the first derived public key to obtain first encrypted service data, wherein the encrypted service data comprises the first encrypted service data;
encrypting the service data by using an encryption key to obtain second
30 encrypted service data; and
encrypting a decryption key corresponding to the encryption key by using the first derived key to obtain encrypted key data, wherein the encrypted service data comprises the second encrypted service data and the encrypted key data; and

sending the encrypted service data to the blockchain, so that the encrypted service data is recorded in the distributed database of the blockchain after the blockchain performs consensus verification on the encrypted service data.

- 5 7. The non-transitory, computer-readable medium of claim 6, the operations further comprising:

 sending a request transaction for the first derived private key to the blockchain, wherein the request transaction is encrypted by the user private key of the key receiver, so that the node device of the key distributor sends the first derived private key encrypted by the user public
10 key of the key receiver to the blockchain after successfully verifying the request transaction based on the user public key of the key receiver.

8. The non-transitory, computer-readable medium of claim 6, wherein the first derived key is a key derived from the derived key of the key distributor through key derivation function
15 (KDF) calculation based on a service data access permission type of the key receiver.

9. The non-transitory, computer-readable medium of claim 6, the operations further comprising:

 storing the first derived key and an identifier of the service data permission type in a
20 local database of the key receiver.

10. The non-transitory, computer-readable medium of claim 9, wherein the sending the encrypted service data to the blockchain comprises:

 sending the encrypted service data and the identifier of the service data permission type
25 to the blockchain.

11. A computer-implemented system, comprising:

 one or more computers; and

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

 obtaining, by a node device of a key receiver, a first derived key that is distributed by a node device of a key distributor, wherein the first derived key is derived from a derived key of

the key distributor based on a service data permission type of the key receiver, wherein both the derived key of the key distributor and the first derived key are asymmetric encryption key pairs, and the first derived key comprises a first derived public key and a first derived private key, wherein obtaining the first derived key comprises obtaining, by the node device of the key receiver, the first derived public key and the first derived private key encrypted by a user public key of the key receiver from a distributed database of a blockchain;

encrypting service data based on the first derived key to obtain encrypted service data, comprising:

encrypting the service data by using the first derived public key to obtain first encrypted service data, wherein the encrypted service data comprises the first encrypted service data;

encrypting the service data by using an encryption key to obtain second encrypted service data; and

encrypting a decryption key corresponding to the encryption key by using the first derived key to obtain encrypted key data, wherein the encrypted service data comprises the second encrypted service data and the encrypted key data; and

sending the encrypted service data to the blockchain, so that the encrypted service data is recorded in the distributed database of the blockchain after the blockchain performs consensus verification on the encrypted service data.

12. The computer-implemented system of claim 11, wherein the one or more operations further comprise:

sending a request transaction for the first derived private key to the blockchain, wherein the request transaction is encrypted by the user private key of the key receiver, so that the node device of the key distributor sends the first derived private key encrypted by the user public key of the key receiver to the blockchain after successfully verifying the request transaction based on the user public key of the key receiver.

13. The computer-implemented system of claim 11, wherein the first derived key is a key derived from the derived key of the key distributor through key derivation function (KDF) calculation based on a service data access permission type of the key receiver.

14. The computer-implemented system of claim 11, wherein the one or more operations further comprise:

storing the first derived key and an identifier of the service data permission type in a local database of the key receiver.

15. The computer-implemented system of claim 14, wherein the sending the encrypted
5 service data to the blockchain comprises:
sending the encrypted service data and the identifier of the service data permission type to the blockchain.