

CLAIMS

~~What is claimed is:~~

1. ~~_____~~ A ~~blockchain-based service data encryption~~ computer-implemented method, ~~applied to~~
5 ~~a blockchain comprising a node device of a key distributor and:~~
~~obtaining, by~~ a node device of a key receiver, ~~comprising:~~
~~obtaining, by the node device of the key receiver,~~ a first derived key that is distributed
by ~~the~~ node device of ~~the~~ 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,
10 ~~and the derived key can decrypt service data encrypted by the first derived key; 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~~
15 ~~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~~
20 ~~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~~
25 ~~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 ~~a~~the distributed database of the blockchain after the blockchain performs
consensus verification on the encrypted service data.
2. ~~The method according to claim 1, wherein both the derived key of the key distributor~~
30 ~~and the first derived key of the key receiver are symmetric encryption keys, and the obtaining,~~
~~by the node device of the key receiver, a first derived key distributed by the node device of the~~
~~key distributor comprises:~~

~~obtaining, by the node device of the key receiver, an encrypted first derived key from the distributed database of the blockchain, wherein the first derived key is encrypted based on a user public key of the key receiver; and~~

~~decrypting the encrypted first derived key based on the user private key of the key receiver to obtain the first derived key.~~

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

~~3. The method according to claim 1, wherein both the derived key of the key distributor and the first derived key of the key receiver are asymmetric encryption key pairs, and the first derived key comprises a first derived public key and a first derived private key; and~~

~~the obtaining, by the node device of the key receiver, a first derived key distributed by the node device of the key distributor comprises:~~

~~obtaining, by the node device of the key receiver, the first derived public key and the first derived private key encrypted by the user public key of the key receiver from the distributed database of the blockchain.~~

~~4. The method according to claim 3, 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. 5. The computer-implemented method according to of claim 1, wherein the first derived key is a key derived from the derived key of the key distributor through KDFkey derivation function (KDF) calculation based on a service data access permission type of the key receiver.~~

~~6.~~

~~4. The method according to claim 2, wherein the encrypting service data based on the first derived key to obtain encrypted service data comprises:~~

~~encrypting the service data by using the first derived key to obtain first encrypted service data, wherein~~

~~the encrypted service data comprises the first encrypted service data of~~

~~7. The method according to claim 3, wherein the encrypting service data based on the first derived key to obtain encrypted service data comprises:~~

~~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.~~

5 ~~8. The method according to claim 2, wherein the encrypting service data based on the first derived key to obtain encrypted service data comprises:~~

~~encrypting the service data by using a third encrypted key to obtain second encrypted service data; and~~

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

~~9. The method according to claim 3, wherein the encrypting service data based on the first derived key to obtain encrypted service data comprises:~~

15 ~~encrypting the service data by using a third encrypted key to obtain second encrypted service data; and~~

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

20 ~~10. The method according to~~ 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.~~

25 5. 11. The method according to claim 104, 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.

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

30

6. 12. A blockchain-based service data encryption apparatus, applied to non-transitory, computer-readable medium storing one or more instructions executable by a

~~blockchain computer system to perform operations comprising a node device of a key distributor and;~~

~~obtaining, by a node device of a key receiver, comprising:~~

~~an obtaining unit, configured to obtain, by the node device of the key receiver, a first~~
5 ~~derived key that is distributed by the node device of the 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, and wherein both the derived key can decrypt service data~~
~~encrypted by of the key distributor and the first derived key; are asymmetric encryption key~~
10 ~~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;~~

~~an encryption unit, configured to encrypt encrypting service data based on the first~~
~~derived key to obtain encrypted service data; and, comprising:~~

15 ~~a sending unit, configured 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~~

20 ~~encrypting a decryption key corresponding to the encryption key by using the~~
~~first derived key to send 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~~
25 ~~consensus verification on the encrypted service data.~~

7. 13. ~~The apparatus according to claim 12, wherein both the derived key of the key~~
~~distributor and the first derived key of the key receiver are symmetric encryption keys, and the~~
~~obtaining unit is configured to:~~

30 ~~obtain, by the node device of the key receiver, an encrypted first derived key from the~~
~~distributed database of the blockchain, wherein the first derived key is encrypted based on a~~
~~user public key of the key receiver; and~~

~~decrypt the encrypted first derived key based on the user private key of the key receiver to obtain the first derived key. The non-transitory, computer-readable medium of claim 6, the operations further comprising:~~

~~sending~~

5 ~~14. The apparatus according to claim 12, wherein both the derived key of the key distributor and the first derived key of the key receiver are asymmetric encryption key pairs, and the first derived key comprises a first derived public key and a first derived private key; and~~

~~the obtaining unit is configured to:~~

10 ~~obtain the first derived public key and the first derived private key encrypted by the user public key of the key receiver from the distributed database of the blockchain.~~

~~15. The apparatus according to claim 14, wherein the sending unit is configured to:~~

15 ~~send~~ 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.

20 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 (KDF) calculation based on a service data access permission type of the key receiver.

25 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 local database of the key receiver.

30 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 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 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

5 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

10 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,

15 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

20 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

25 is recorded in the distributed database of the blockchain after the blockchain performs consensus verification on the encrypted service data.

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

30 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.

5 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 KDFkey derivation function (KDF) calculation based on a service data access permission type of the key receiver.

10 ~~14. 17. The apparatus according to computer-implemented system of claim 1311,~~
wherein the ~~encryption unit is configured to:~~
~~encrypt the service data by using the first derived key to obtain first encrypted service data, wherein~~

~~the encrypted service data comprises the first encrypted service data.~~

~~18. The apparatus according to claim 14, wherein the encryption unit is configured to:~~
~~encrypt the service data by using the first derived public key to obtain first encrypted~~
15 ~~service data, wherein~~

~~the encrypted service data comprises the first encrypted service data.~~

~~19. The apparatus according to claim 13, wherein the encryption unit is configured to:~~
~~encrypt the service data by using a third encrypted key to obtain second encrypted service~~
20 ~~data; and~~

~~encrypt a third decryption key corresponding to the third encryption key by using the first~~
20 ~~derived key to obtain third encrypted key data, wherein~~

~~the encrypted service data comprises the second encrypted service data and the third encrypted key data.~~

~~20. The apparatus according to claim 14, wherein the encryption unit is configured to:~~
25 ~~encrypt the service data by using a third encrypted key to obtain second encrypted service~~
~~data; and~~

~~encrypt a third decryption key corresponding to the third encryption key by using the first~~
~~derived public key to obtain third encrypted key data, wherein~~

~~the encrypted service data comprises the second encrypted service data and the third~~
30 ~~encrypted key data.~~

~~21. The apparatus according to claim 12, one or more operations further comprising:comprise:~~
~~a storage unit, configured to store~~storing the first derived key and an identifier of the
service data permission type in a local database of the key receiver.

~~15. 22.~~ _____ The ~~apparatus according to computer-implemented system of claim 21~~14, wherein the sending ~~unit is configured to:~~the encrypted service data to the blockchain comprises:

5 ~~send~~sending the encrypted service data and the identifier of the service data permission type to the blockchain.

~~23. A computer device, comprising a memory and a processor, wherein the memory stores a computer program that can be run by the processor, and the processor performs the method according to any one of claims 1 to 11 when running the computer program.~~