

CLAIMS

What is claimed is:

1. A computer-implemented method for storing blockchain account private keys, comprising:
 - 5 obtaining, performed by a private key management program installed on a user device of a user, wherein the user device stores (i) an encrypted private key set obtained by using a predetermined encryption key to encrypt a private key set provided by the user and (ii) an association relationship between predetermined identification information of the user and the private key set, and wherein the method comprises:
 - 10 obtaining input identification information provided by the user;
determining whether the input identification information matches the predetermined identification information of the user;
in response to determining that the input identification information matches the predetermined identification information of the user, obtaining a decryption key - 15 provided by the user;
determining whether the decryption key provided by the user is associated with the predetermined encryption key; and
in response to determining that both (i) the input identification information matches the predetermined identification information of the user and (ii) the decryption - 20 key provided by the user is associated with the predetermined encryption key, returning the private key set to the user, wherein the private key set is obtained by using the decryption to process the encrypted private key set stored on the user device.
- 25 2. The computer-implemented method according to claim 1, wherein the private key set comprises at least one account private key of a blockchain account registered by the user.
3. The computer-implemented method according to claim 1, wherein the identification
information comprises a mobile number or an identity card number of the user.
30
4. The computer-implemented method according to claim 1, wherein the identification
information comprises biometric identification information of the user, wherein the
biometric identification information comprises fingerprint information or face
information.
35

5. The computer-implemented method according to claim 1, wherein the encrypted private key set is stored on the user device only after obtaining the predetermined identification information provided by the user.

5

6. The computer-implemented method according to claim 1, wherein the predetermined encryption key is an asymmetric key, and wherein determining whether the decryption key provided by the user is associated with the predetermined encryption key comprises processing the encrypted private key set using the decryption key provided by the user.

10

7. The computer-implemented method according to claim 1, wherein the predetermined encryption key is a symmetric key.

8. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to implement a private key management program on a user device of a user, wherein the user device stores (i) an encrypted private key set obtained by using a predetermined encryption key to encrypt a private key set provided by the user and (ii) an association relationship between predetermined identification information of the user and the private key set, and wherein the private key management program is configured to perform operations comprising:

20

obtaining input identification information provided by the user;

determining whether the input identification information matches the predetermined identification information of the user;

in response to determining that the input identification information matches the predetermined identification information of the user, obtaining a decryption key provided by the user;

25

determining whether the decryption key provided by the user is associated with the predetermined encryption key; and

in response to determining that both (i) the input identification information matches the predetermined identification information of the user and (ii) the decryption key provided by the user is associated with the predetermined encryption key, returning the private key set to the user, wherein the private key set is obtained by using the decryption to process the encrypted private key set stored on the user device.

30

35

9. The non-transitory, computer-readable medium according to claim 8, wherein the private key set comprises at least one account private key of a blockchain account registered by the user.

~~obtaining an encryption key provided by the user; and~~

~~encrypting the private key set by using the encryption key, and storing the encrypted private key set.~~

~~2~~

5 ~~10. The method~~non-transitory, computer-readable medium according to claim 4, wherein the private key set further comprises an account private key provided by at least one other user to the user; and for each other user, the account private key provided by the other user to the user is an account private key of a blockchain account registered by the other user;~~8, wherein the~~

10 ~~3.~~The method according to claim 1, wherein the method further comprises:

~~obtaining identification information provided by~~comprises a mobile number or an identity card number of the user; and,

15 ~~11. establishing and storing an association relationship between the~~The non-transitory, computer-readable medium according to claim 8, wherein the identification information ~~and the private key set.~~comprises biometric

~~4.~~The method according to claim 3, wherein the storing the encrypted private key set specifically comprises:

20 ~~after obtaining the~~ identification information provided by the user, storing the encrypted private key set.

~~5.~~A method for invoking the account private keys stored based on the method according to any one of claims 1 to 4, comprising:

~~obtaining, by a private key management program, a decryption key provided by the user;~~

25 ~~decrypting the encrypted private key set by using the decryption key; and~~
~~returning the decrypted private key set to the user.~~

~~6.~~The method according to claim 5, wherein before the decrypting the encrypted private key set by using the decryption key, the method further comprises:

~~obtaining~~the biometric identification information ~~provided by the user; and~~

~~determining whether the identification comprises fingerprint information provided by the user matches the identification or face information associated with the private key set; and,~~

5 12. the decrypting ~~The non-transitory, computer-readable medium according to claim 8, wherein~~ the encrypted private key set ~~by using~~ is stored on the user device only after obtaining the decryption key specifically comprises:

~~if the predetermined~~ identification information provided by the user ~~matches the identification information associated with the private key set, decrypting the encrypted private key set by using the decryption key; or,~~

10

13. if the identification information provided by the user does not match the identification information associated with the private key set, refusing ~~The non-transitory, computer-readable medium according to decrypt~~ claim 8, wherein the predetermined encryption key is an asymmetric key, and wherein determining whether the decryption key provided by the user is associated with the predetermined encryption key comprises processing the encrypted private key set ~~by using~~ the decryption key provided by the user.

15

~~7. An apparatus for storing blockchain account private keys~~

20 14. The non-transitory, computer-readable medium according to claim 8, wherein the apparatus predetermined encryption key is installed a symmetric encryption key.

15. A computer-implemented system, comprising:

one or more computers; and

25 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, implement a private key management program on a user device of a user, and the apparatus comprises; wherein the user device stores (i) an encrypted private key set obtained by using a predetermined encryption key to encrypt a private key set provided by the user

30 and (ii) an association relationship between predetermined identification information of the user and the private key set, and wherein the private key management program is configured to perform operations comprising:

35 a first acquisition module, configured to obtain a private key set; obtaining input identification information provided by the user;

determining whether the input identification information matches the predetermined identification information of the user;

in response to determining that the input identification information matches the predetermined identification information of the user, obtaining a decryption key provided by the user;

determining whether the decryption key provided by the user is associated with the predetermined encryption key; and

in response to determining that both (i) the input identification information matches the predetermined identification information of the user and (ii) the decryption key provided by the user is associated with the predetermined encryption key, returning the private key set to the user, wherein the private key set is obtained by using the decryption to process the encrypted private key set stored on the user device.

16. The computer-implemented system according to claim 15, wherein the private key set comprises at least one account private key of a blockchain account registered by the user;

~~a second acquisition module, configured to obtain an encryption key provided by the user; and~~

~~an encryption and storage module, configured to encrypt the private key set by using the encryption key, and store the encrypted private key set.~~

~~8~~

17. The apparatus~~computer-implemented system~~ according to claim 7, wherein the private key set further comprises an account private key provided by at least one other user to the user; and for each other user, the account private key provided by the other user to the user is an account private key of a blockchain account registered by the other user.

9. The apparatus according to claim 7, wherein the apparatus further comprises:

~~a third acquisition module, configured to obtain~~ 15, wherein the identification information provided by~~comprises a mobile number or an identity card number of the user; and establish and store an association relationship between.~~

18. The computer-implemented system according to claim 15, wherein the identification information ~~and the private key set.~~

~~10. The apparatus according to claim 9, wherein after the~~comprises biometric identification information provided by the user is obtained, the encryption and storage module stores the encrypted private key set.

~~11. An apparatus for invoking the account private keys stored based on the~~
5 ~~apparatus according to any one of claims 7 to 10, wherein the apparatus is installed on the user device of the user, and the apparatus comprises:~~

~~an acquisition module, configured to obtain a decryption key provided by the user;~~

~~a decryption module, configured to decrypt the encrypted private key set by~~
10 ~~using the decryption key; and~~

~~a returning module, configured to return the decrypted private key set to the user.~~the user, wherein the biometric

~~12. The apparatus according to claim 11, wherein the apparatus further comprises: an identity verification module, configured to, before the encrypted private key set is~~
15 ~~decrypted by using the decryption key, obtain identification information provided by the user; and determine whether the identification~~comprises fingerprint ~~information provided by the user matches the identification~~or face ~~information associated with the private key set; and,~~

~~the decryption module is configured to, if the identity verification module determines that the~~
20

~~19. The computer-implemented system according to claim 15, wherein the encrypted private key set is stored on the user device only after obtaining the predetermined identification information provided by the user~~matches the identification information associated with the private key set, decrypt the encrypted private key set by using the
25 ~~decryption key; or,~~

~~if~~

~~20. The computer-implemented system according to claim 15, wherein the identity verification module determines that the identification information~~predetermined encryption key is an asymmetric key, and wherein determining whether the decryption
30 ~~key provided by the user does not match the identification information~~is associated with the private key set, refuse to decryptpredetermined encryption key comprises processing the encrypted private key set by using the decryption keyprovided by the user.

~~21. The computer-implemented system according to claim 15, wherein the predetermined encryption key is a symmetric encryption key.~~13. A computer device,

~~comprising a memory, a processor, and a computer program that is stored in the memory and that can run on the processor, wherein when executing the program, the processor implements the method according to any one of claims 1 to 6.~~