CLAIMS

What is claimed is:

1. A computer-implemented method 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:

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.

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.

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.

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.

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.

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:

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.

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.

10. The non-transitory, computer-readable medium according to claim 8, wherein the identification information comprises a mobile number or an identity card number of the user.

11. The non-transitory, computer-readable medium according to claim 8, wherein the identification information comprises biometric identification information of the user, wherein the biometric identification information comprises fingerprint information or face information.

12. The non-transitory, computer-readable medium according to claim 8, wherein the encrypted private key set is stored on the user device only after obtaining the predetermined identification information provided by the user.

13. The non-transitory, computer-readable medium according to 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 using the decryption key provided by the user.

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

15. 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, 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:

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.

17. The computer-implemented system according to claim 15, wherein the identification information comprises a mobile number or an identity card number of the user.

18. The computer-implemented system according to claim 15, wherein the identification information comprises biometric identification information of the user, wherein the biometric identification information comprises fingerprint information or face information.

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.

20. The computer-implemented system according to claim 15, 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.

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