

CLAIMS

1. A computer-implemented method for managing a cryptographic key, the method comprising:

receiving a request for a signature on transaction data;

allocating a key manager corresponding to the request; and

obtaining, by the key manager, the signature on the transaction data and the cryptographic key, wherein the cryptographic key is a public key, and the signature on the transaction data is obtained based on a private key corresponding to the public key.

2. The method of claim 1, wherein allocating the key manager corresponding to the request further comprises:

determining whether the request includes internal account information; and

in response to a determination that the request includes the internal account information, allocating a first key manager that generates the cryptographic key.

3. The method of claim 2, wherein allocating the key manager corresponding to the request further comprises:

in response to a determination that the request does not include the internal account information, determining whether the request includes bank account information; and

in response to a determination that the request includes the bank account information, allocating a second key manager that obtains the signature on the transaction data and the cryptographic key from a bank.

4. The method of claim 3, wherein allocating the key manager corresponding to the request further comprises:

in response to a determination that the request does not include the bank account information, determining whether the request includes information of an independent enterprise that owns a cryptographic management system; and

in response to a determination that the request includes the information of the independent enterprise, allocating a third key manager that obtains the signature on the transaction data and the cryptographic key from the independent enterprise.

5. The method of claim 4, wherein allocating the key manager corresponding to the request further comprises:

in response to a determination that the request does not include the information of the independent enterprise, allocating a fourth key manager that obtains the cryptographic key from a key management service.

6. The method of any preceding claim, further comprising:
reformatting the obtained signature on the transaction data.

7. The method of any preceding claim, further comprising:
broadcasting the obtained signature on the transaction data and the obtained cryptographic key; and
updating a member account database.

8. The method of claim 7, further comprising:
identifying and registering an overtime task,
wherein the overtime task occurs when the signature on the transaction data is not obtained within a predetermined time period.
9. The method of claim 3, wherein the second key manager obtains the signature on the transaction data and the cryptographic key from the bank using a USB key of a user.
10. The method of claim 4, wherein the third key manager obtains the signature on the transaction data and the cryptographic key from the independent enterprise through an application programming interface connector.
11. The method of any preceding claim, further comprising:
creating an account in a blockchain system; and
uploading the obtained signature on the transaction data to the blockchain system for verification.
12. The method of any preceding claim, wherein allocating the key manager corresponding to the request is performed based on an idempotent control protocol.
13. A device for managing cryptographic keys, comprising:
one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 12.

14. An apparatus for managing cryptographic keys, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 12.

15. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 to 12.