

CLAIMS

1. A computer-implemented method for managing a cryptographic key to create an account in a blockchain system, the method comprising:

receiving a request for a signature on transaction data;

allocating a key manager corresponding to the request; ~~and~~, comprising:

determining whether the request includes internal testing account information;

in response to a determination that the request includes the internal testing account information, allocating a first key manager that is to generate the cryptographic key;

in response to a determination that the request does not include the internal testing 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 is to obtain the signature on the transaction data and the cryptographic key from a bank; and

obtaining, by the allocated 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;~~ wherein obtaining, by the allocated key manager, the signature on the transaction data and the cryptographic key comprises:

generating, by the allocated key manager, a mock cryptographic key as the cryptographic key and obtaining, by the allocated key manager, a mock signature on the transaction data as the signature on the transaction data when the allocated key manager is the first key manager, and

obtaining, by the allocated key manager, the signature on the transaction data and the cryptographic key from the bank when the allocated key manager is the second key manager.

~~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.~~

24. The method of claim 13, 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.

[35](#). The method of claim [24](#), 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.

[64](#). The method of any preceding claim, further comprising:
reformatting the obtained signature on the transaction data.

[75](#). 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.

[86](#). The method of claim [75](#), 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.

[97](#). The method of claim [31](#), 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.

~~408.~~ The method of claim ~~42~~, 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.

~~449.~~ 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.

~~4210.~~ The method of any preceding claim, wherein allocating the key manager corresponding to the request is performed based on an idempotent control protocol.

~~4311.~~ 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 ~~4210~~.

~~14.—An apparatus~~~~12.~~ A computer program product for managing cryptographic keys, the ~~apparatus~~~~computer program product~~ comprising ~~a plurality~~~~instructions which, when executed by one or more processors~~ of ~~modules for performing~~a device, cause the one or more processors to perform the method of any of claims 1 to ~~4210~~.

~~45~~13. A non-transitory computer-readable medium having stored therein instructions that, when executed by ~~a processor~~one or more processors of a device, cause the ~~device~~one or more processors to perform the method of any of claims 1 to ~~42~~10.