

~~I/We Claim~~ **CLAIMS:**

1. A method of key management, comprising:

obtaining, at a user device of a primary user for splitting a transaction key, a number of users in a group of users for managing the transaction key and a first predetermined value, the first predetermined value indicating a minimum number of users in the group of users for restoring the transaction key;

randomly generating, at the user device of the primary user, based on a message from a management device related to a further user in the group of users, the transaction key, wherein the transaction key is associated with processing a permission of a present transaction, wherein the message includes at least a public key of the further user;

at the user device of the primary user, splitting the transaction key into a plurality of sub-keys, the number of sub-keys being the same as the number of users; and

at the user device of the primary user, encrypting each of the plurality of sub-keys with a public key of a corresponding one of the users in the group of users associated with a given sub-key; and

sending the plurality of encrypted sub-keys from the user device of the primary user to the management device.

2. The method of claim 1, wherein the primary user is specified or randomly determined from the group of users by the management device.

3. The method of claim 1, wherein the message from the management device related to the further user indicates at least one of:

a credential of the management device;

signature information for verifying the public key of the further user;

an identification of the further user;

signature information of a hash value of merged data of the further user; and

a validity period of the message.

4. The method of claim 3, wherein randomly generating the transaction key comprises:

in response to determining that the credential of the management device is valid, determining, based on the signature information of the public key of the further user, whether

the public key of the further user is valid; and

in response to the public key of the further user being valid, randomly generating a plurality of random numbers for building a splitting polynomial, the number of random numbers being the same as the first predetermined value, the plurality of random numbers for building the splitting polynomial comprising the transaction key.

5. The method of claim 4, wherein splitting the transaction key into the plurality of sub-keys comprises:

determining, based on the number of users in the group of users and the plurality of random numbers for building the splitting polynomial, the plurality of sub-keys, each of the plurality of sub-keys comprising first sub-key data and second sub-key data.

6. The method of claim 1, wherein the step of encrypting further comprises:
encrypting the sub-key based on the public key of the user corresponding to the sub-key and a validity period of the message related to the further user.

7. The method of claim 1, further comprising:
in response to determining that signature data from the management device is valid, signing the signature data based on a private key preset in the user device, the signature data comprising at least a random number signed by the management device; and

in response to a user being determined as an organizing primary user for organizing the group of users, sending, to the management device, group information about the group of users, a public key of the user device of the organizing primary user and the signature data signed with a private key of the user device of the organizing primary user, the group information comprising at least the number of users in the group of users and the first predetermined value.

8. The method of claim 1, wherein the user device comprises a hardware USB key with a processing unit.

~~9. A method of key management among a group of users, comprising:
in response to a user from the group of users being determined as a restoring user for restoring a transaction key, obtaining, at a user device of the restoring user, a restoration message from a management device for restoring the transaction key, the restoration message indicating at least a number of confirming users in the group of users and an identification of~~

~~the restoring user, the confirming users approving a present transaction;~~

~~in response to determining that the number of confirming users is larger than or equal to a first predetermined value, determining the transaction key based on sub-keys of the confirming users obtained from the management device, wherein the sub-keys of the confirming users were generated by splitting the transaction key in advance; and~~

~~signing a transaction request for the present transaction based on the determined transaction key.~~

~~10. The method of claim 9, wherein the restoring user is specified or randomly determined by the management device from the group of users.~~

~~11. The method of claim 9, wherein the sub-keys of the confirming users were sent by the confirming users to the management device, and the sub-keys of the confirming users are encrypted with a public key of the restoring user.~~

~~12. The method of claim 11, wherein the sub-keys of the confirming users were encrypted at the user devices of the confirming users with the public key of the restoring user obtained via the management device and a present transaction random number associated with the present transaction.~~

~~13. The method of claim 9, wherein the restoration message further indicates at least one of:
a present transaction random number associated with the present transaction;
the sub-keys of the confirming users and the present transaction random number signed with a public key of the restoring user;
signature information of the confirming users;
a credential of the management device; and
signature information of a hash value of the restoration message.~~

~~14. 9. A method of key management with a group of users, the group of users including an organizing primary user for creating the group of users and a primary user for splitting a transaction key, the method comprising:
obtaining, at a management device, group information about the group of users from a user device of the organizing primary user, the group information indicating at least the number~~

of users in the group of users and a first predetermined value, the first predetermined value indicating the minimum number of users for restoring a transaction key, the group of users being used to manage the transaction key;

sending a message to a user device of the primary user for splitting the transaction key, wherein the message is related to a first one of the users in the group of users other than the primary user for splitting the transaction key, wherein the message indicates at least a public key of the first one of the users;

obtaining a plurality of sub-keys from the primary user for splitting the transaction key, the number of sub-keys being the same as the number of users in the group of users, wherein the plurality of sub-keys were generated by the primary user for splitting the transaction key by randomly generating the transaction key and then splitting the transaction key, the plurality of sub-keys being encrypted with public keys of the respective users; and

caching the plurality of sub-keys for sending to the respective users.

~~15.~~ 10. The method of claim ~~14~~9, further comprising:

specifying or randomly determining, in the group of users, at least one of:

at least one of the organizing primary user and the primary user for splitting the transaction key; and

a restoring user for restoring the transaction key.

~~16~~11. The method of claim ~~15~~10, further comprising:

in response to receiving a request for a present transaction, sending, to users of the group of users, transaction information for determining whether the present transaction is approved, the transaction information indicating at least transaction content of the present transaction and an identification of the restoring user;

obtaining a sub-key of each confirming user in the group of users, the confirming user approving the present transaction, the sub-keys of the confirming users being signed with a public key of the restoring user; and

in response to determining that a condition for the present transaction is satisfied, sending, to the restoring user, a restoration message for restoring the transaction key.

~~17.~~ 12. The method of claim ~~9~~14, further comprising:

in response to a registration request from a user device of a user in the group of users, sending signature data of the management device to the user device, the signature data

comprising at least a random number signed by the management device;

determining, based on signature data from the user device, whether the user device is valid, the signature data being generated by signing the random number by the user device based on a private key preset in the user device in response to determining that the management device is valid; and

in response to determining that a user device of each user in the group of users is valid, determining that the group of users is valid.

~~18~~13. The method of claim ~~14~~9, wherein the user device comprises a hardware USB key with a processing unit.

~~19~~. 14. A user device for key management, comprising:
a memory configured to store one or more computer programs; and
a processing unit coupled to the memory and configured to execute the one or more computer programs to cause the device to perform a method according to any of claims 1 to ~~13~~8.

~~20~~. 15. A management device for key management, comprising:
a memory configured to store one or more computer programs; and
a processing unit coupled to the memory and configured to execute the one or more computer programs to cause the device to perform a method according to any of claims ~~14~~9 to ~~18~~13.

~~21~~. ~~A non-transient computer-readable storage medium comprising machine-executable instructions stored thereon, the machine-executable instructions, when executed, causing a machine to perform steps of a method according to any of claims 1 to 18.~~

~~22~~. ~~A computer program product tangibly stored on a non-transient computer-readable medium and comprising machine-executable instructions, the machine-executable instructions, when executed, causing a machine to perform steps of a method according to any of claims 1 to 18.~~