

CLAIMS

What is claimed is:

1. A blockchain-based ~~resource transfer~~ method for information masking, comprising:
determining, at a computer device of a borrower, according to an agreement with a
5 lender, when a resource transfer condition is met, a first amount of capital to be transferred to
the borrower from the lender ~~to be transferred first resource~~;

determining, at the computer device of the borrower, according to the first amount of ~~the~~
first resource capital, a value number of a second amount of a token based on an output of a
10 function relationship that uses a value number of the first amount of the capital and a random
number as input ~~to be transferred second resource~~, wherein a resource type of the capital first
resource is different from a resource type of the ~~second resource~~ token;

encrypting, at the computer device of the borrower, using a public key of the lender, the
random number to obtain an encrypted random number;

encrypting, at the computer device of the borrower, the value number of the second
15 amount of the token using the public key of the lender and a first encryption function to obtain
first encrypted amount information; and

initiating, at the computer device of the borrower, by a resource transferor, a transaction
request to a blockchain to transfer the ~~to be transferred second~~ amount of the token from the
borrower to the lender ~~resource to a resource transferee~~, wherein the transaction request
20 comprises the encrypted random number, the first encrypted amount information, and a
zero-knowledge proof that the value number of the second amount is less than a value number
of an original amount of the token of the borrower, the value number of the second amount is
positive, and the value number of the original amount is positive ~~first encrypted amount~~
~~information obtained after the second amount of the second resource is encrypted~~; and

25 ~~executing, after the blockchain verifies the transaction request, the transaction request to~~
~~transfer the to be transferred second resource to the resource transferee, and~~
~~recording an execution result on the blockchain.~~

2. The method according to claim 1, further comprising:

30 after the transaction request is executed and recorded to the blockchain, obtaining, at a
computer device of the lender, the encrypted random number from the blockchain;

determining, at the computer device of the lender, the random number based on the
encrypted random number and a private key of the lender;

35 determining, at the computer device of the lender, the value number of the first amount
of the capital based on the determined random number and the function relationship according
to reverse conversion;

after the second amount of the token is transferred to the lender, sending off the blockchain, at the computer device of the lender to the borrower, the first amount of the capital;

receiving off the blockchain, at the computer device of the lender from the borrower, the first amount of the capital; and

in response to receiving the first amount of the capital, initiating, at the computer device of the lender, a different transaction request to the blockchain to transfer the second amount of the token from the lender to the borrower.

~~2. The method according to claim 1, wherein the first encrypted amount information in the transaction request is obtained by encrypting the second amount of the second resource using a first encryption function, wherein~~

~~an input of the first encryption function is the second amount of the second resource, and another input of the first encryption function is a public key of the resource transferee.~~

~~3. The method according to claim 2, wherein determining the value number of the second amount of the token comprises:~~

~~inputting, at the computer device of the borrower, the value number of the first amount of the capital and the random number into the function relationship to output the value number of the second amount of the token.~~

~~4. The method according to claim 1, wherein the value number of the first amount of the capital and the resource type of the capital are unknown to the blockchain.~~

~~35. The method according to claim 21, wherein the transaction request further comprises a hash value of the public key of the lender and a hash value of a blockchain transaction stored on the blockchain recording the original amount of the token of the borrower; identification information of the public key of the resource transferee.~~

~~6. The method according to claim 5, wherein the transaction request further comprises: an encryption of the amount value of the original amount based on a public key of the borrower; and a hash value of a public key of the borrower.~~

~~4. The method according to claim 3, wherein the identification information of the public key of the resource transferee is a hash value of the public key of the resource transferee.~~

~~5. The method according to claim 1, wherein the determining, according to the first~~

~~amount of the first resource, a second amount of a to be transferred second resource comprises:~~

~~determining, according to the first amount of the first resource, the second amount of the second resource using a one way function.~~

5

~~6. The method according to claim 5, wherein the determining the second amount of the second resource using a one way function comprises:~~

~~using the first amount of the first resource and a random number as inputs of the one way function, and~~

10

~~determining an output of the one way function as the second amount of the second resource.~~

~~7. The method according to claim 6, wherein the transaction request initiated by the resource transferor to the blockchain further comprises an encrypted random number generated by encrypting the random number.~~

15

~~8. The method according to any one of claims 1 to 7, wherein:~~

~~the resource transfer condition comprises allowing the resource transferee to borrow the first resource, and~~

20

~~the determining a first amount of a to be transferred first resource comprises:~~

~~using a credit limit of an allowed first resource borrowed from the resource transferee as the first amount of the to be transferred first resource.~~

~~9. The method according to any one of claims 1 to 7, wherein~~

25

~~the resource transfer condition comprises that the resource transferor has received the first resource returned by the resource transferee, and~~

~~the determining a first amount of a to be transferred first resource comprises:~~

~~determining an amount of the returned first resource as the first amount of the to be transferred first resource.~~

30

~~10. The method according to any one of claims 1 to 7, wherein:~~

~~the resource transfer condition comprises that the resource transferee and the resource transferor reach a resource borrowing agreement, wherein the resource borrowing agreement comprises an amount of a first resource that the resource transferor requests to borrow from the resource transferee; and~~

35

~~the determining a first amount of a to be transferred first resource comprises:~~

~~determining the amount of the first resource that is requested to borrow as the first~~

~~amount of the to be transferred first resource.~~

~~117.~~ The method according to claim ~~405~~, wherein:

~~the transaction request further comprises at the zero-knowledge proof indicates that the value number of the original amount is equal to , used for proving that a sum of the value number of the second amount and a value number of a balance of the second resource token to be held by the resource transferor/borrower after the an execution of the transaction request is equal to an amount of the second resource held by the resource transferor before the transaction request is initiated.~~

~~12.~~ The method according to claim 11, wherein the zero-knowledge proof is further used for proving that the second amount is greater than zero, an amount of the second resource held by the resource transferor before the transaction request is initiated is greater than zero, and the balance of the second resource to be held by the resource transferor after the execution of the transaction request is not less than zero.

~~13.~~ The method according to claim 10, wherein the transaction request further comprises identification information of a previous resource transfer transaction in which the resource transferor participates.

~~14.~~ The method according to claim 13, wherein the identification information of the previous resource transfer transaction in which the resource transferor participates is specifically a hash value that is of the previous resource transfer transaction and that is recorded in the blockchain.

~~15.~~ The method according to claim 10, wherein the transaction request further comprises second encrypted amount information obtained after a balance of the second resource to be held by the resource transferor after the execution of the transaction request is encrypted.

~~168.~~ The method according to claim ~~455~~, further comprising:

~~wherein the second encrypted amount information in the transaction request is obtained by encrypting, at the computer device of the borrower, using a second encryption function, the a balance of the second resource token to be held by the resource transferor/borrower after the an execution of the transaction request to obtain second encrypted amount information,~~ wherein an input of the second encryption function is the balance of the ~~second resource token~~, and another input of the second encryption function is a public key of the ~~resource transferor/borrower~~; and

wherein the transaction request further comprises the second encrypted amount information and a hash value of the public key of the borrower.

~~17. The method according to claim 16, wherein the transaction request further comprises identification information of the public key of the resource transferor.~~

~~18. The method according to claim 17, wherein the identification information of the public key of the resource transferor is a hash value of the public key of the resource transferor.~~

~~19. The method according to any one of claims 1 to 7, or 11 to 18, wherein the first resource is capital, and the second resource is a token.~~

~~20. A blockchain-based capital transfer method, comprising:
determining, when a transfer condition is met, a first amount of to be transferred capital;
determining, according to the first amount of the capital, a second amount of a to be transferred token, wherein a type of the capital is different from a type of the token;
initiating, by a transferor, a transaction request to a blockchain to transfer the to be transferred token to a transferee, wherein the transaction request comprises first encrypted amount information obtained after the second amount of the token is encrypted; and
executing, after the blockchain verifies the transaction request, the transaction request to transfer the to be transferred token to the transferee, and
recording an execution result on the blockchain.~~

~~21. A blockchain-based resource transfer method, comprising:
determining, when a resource transfer condition is met, a first amount of a to be transferred first resource;
determining, according to the first amount of the first resource, a second amount of a to be transferred second resource using a one way function, wherein a type of the first resource is different from a type of the second resource;
initiating, by a resource transferor, a transaction request to a blockchain to transfer the to be transferred second resource to a resource transferee, wherein the transaction request comprises information corresponding to the second amount of the second resource; and
executing, after the blockchain verifies the transaction request, the transaction request to transfer the to be transferred second resource to the resource transferee, and
recording an execution result in the blockchain.~~

~~22. A blockchain-based capital transfer method, comprising:
determining, when a transfer condition is met, a first amount of to be transferred capital;
determining, according to the first amount of the capital, a second amount of a
to be transferred token using a one way function, wherein a type of the capital is different
from a type of the token;
initiating, by a transferor, a transaction request to a blockchain to transfer the
to be transferred token to a transferee, wherein the transaction request comprises information
corresponding to the second amount of the token; and
executing, after the blockchain verifies the transaction request, the transaction request to
transfer the to be transferred token to the transferee, and
recording an execution result on the blockchain.~~

9. A system, comprising:
one or more processors; and
one or more memories configured to store instructions executable by the one or more
processors to cause the one or more processors to perform operations comprising:
determining, at a computer device of a borrower, according to an agreement with a lender,
a first amount of capital to be transferred to the borrower from the lender;
determining, at the computer device of the borrower, according to the first amount of
capital, a value number of a second amount of a token based on an output of a function
relationship that uses a value number of the first amount of the capital and a random number
as inputs, wherein a resource type of the capital is different from a resource type of the token;
encrypting, at the computer device of the borrower, using a public key of the lender, the
random number to obtain an encrypted random number;
encrypting, at the computer device of the borrower, the value number of the second
amount of the token using the public key of the lender and a first encryption function to obtain
first encrypted amount information; and
initiating, at the computer device of the borrower, a transaction request to a blockchain to
transfer the second amount of the token from the borrower to the lender, wherein the
transaction request comprises the encrypted random number, the first encrypted amount
information, and a zero-knowledge proof that the value number of the second amount is less
than a value number of an original amount of the token of the borrower, the value number of
the second amount is positive, and the value number of the original amount is positive.

10. The system according to claim 9, wherein the one or more processors are further
caused to perform operations comprising:
after the transaction request is executed and recorded to the blockchain, obtaining, at a
computer device of the lender, the encrypted random number from the blockchain;

determining, at the computer device of the lender, the random number based on the encrypted random number and a private key of the lender;

determining, at the computer device of the lender, the value number of the first amount of the capital based on the determined random number and the function relationship according to reverse conversion;

after the second amount of the token is transferred to the lender, sending off the blockchain, at the computer device of the lender to the borrower, the first amount of the capital;

receiving off the blockchain, at the computer device of the lender from the borrower, the first amount of the capital; and

in response to receiving the first amount of the capital, initiating, at the computer device of the lender, a different transaction request to the blockchain to transfer the second amount of the token from the lender to the borrower.

11. The system according to claim 10, wherein determining the value number of the second amount of the token comprises:

inputting, at the computer device of the borrower, the value number of the first amount of the capital and the random number into the function relationship to output the value number of the second amount of the token.

12. The system according to claim 9, wherein the value number of the first amount of the capital and the resource type of the capital are unknown to the blockchain.

13. The system according to claim 9, wherein the transaction request further comprises a hash value of the public key of the lender and a hash value of a blockchain transaction stored on the blockchain recording the original amount of the token of the borrower.

14. The system according to claim 13, wherein the transaction request further comprises: an encryption of the amount value of the original amount based on a public key of the borrower; and

a hash value of a public key of the borrower.

15. The system according to claim 13, wherein:

the zero-knowledge proof indicates that the value number of the original amount is equal to a sum of the value number of the second amount and a value number of a balance of the token to be held by the borrower after an execution of the transaction request.

16. The system according to claim 13, the one or more processors are further caused to perform operations comprising:

encrypting, at the computer device of the borrower, using a second encryption function, a balance of the token to be held by the borrower after an execution of the transaction request to obtain second encrypted amount information, wherein an input of the second encryption function is the balance of the token, and another input of the second encryption function is a public key of the borrower; and

wherein the transaction request further comprises the second encrypted amount information and a hash value of the public key of the borrower.

17. A non-transitory computer-readable storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform one or more steps of a blockchain-based method for information masking according to any one of claims 1 to 8.