

CLAIMS

What is claimed is:

1. A blockchain-based method for information masking, comprising:

determining, at a computer device of a borrower, according to an agreement with a lender,
5 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;

10 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

15 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
20 the second amount is positive, and the value number of the original amount is positive.

2. The method according to claim 1, further 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;

25 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;

30 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

35 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.

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

5 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.

10 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.

15 5. The method according to claim 1, 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.

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.

20 7. The method according to claim 5, 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.

25 8. The method according to claim 5, further 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
30 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.

35 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;

5 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;

10 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

15 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.

20 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;

25 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;

30 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

35 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
5 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.

10 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:
15 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:
20 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
25 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
30 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
35 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.