

CLAIMS

What is claimed is:

1. A blockchain-based resource transfer method, comprising:
determining, when a resource transfer condition is met, a first amount of a
5 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, wherein a type of the first resource is different from a type
of the second resource;
10 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 first encrypted amount information obtained after the second amount of the second
resource is encrypted; and
executing, after the blockchain verifies the transaction request, the transaction request to
15 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, 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
20 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 the transaction request further comprises
identification information of the public key of the resource transferee.
25
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
30 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.
- 35 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

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

5

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.

10

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

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

15

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

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

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

20

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.

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

25

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

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

30

determining the amount of the first resource that is requested to borrow as the first amount of the to-be-transferred first resource.

11. The method according to claim 10, wherein the transaction request further comprises a zero-knowledge proof, used for proving that a sum of the second amount and a balance of the second resource to be held by the resource transferor after the 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.

35

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.

16. The method according to claim 15, wherein the second encrypted amount information in the transaction request is obtained by encrypting, using a second encryption function, the balance of the second resource to be held by the resource transferor after the execution of the transaction request, wherein

an input of the second encryption function is the balance of the second resource, and another input of the second encryption function is a public key of the resource transferor.

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;

5 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

10 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;

15 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
20 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;

30 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

35 recording an execution result on the blockchain.