

CLAIMS

What is claimed is:

1. A blockchain-based remittance method, wherein a remitter account comprises a reserve fund list; and the reserve fund list comprises multiple reserved amounts
5 obtained by dividing a balance of the remitter account; and

the method comprises:

receiving a plurality of remittance transactions, wherein each remittance transaction is sent by a remitter and is used for remittance to a remittee, wherein each remittance transaction comprises a remittance amount that is remitted by the remitter
10 account to a remittee account and at least one reserved amount that corresponds to the remittance amount and that is allocated by the remitter from the reserve fund list to the remittance transaction, wherein at least one of the multiple reserved amounts is allocated to each remittance transaction in the plurality of remittance transactions;

concurrently performing verification on the plurality of remittance transactions,
15 wherein the verification on each remittance transaction comprises determining whether a total reserved amount of the at least one reserved amount comprised in the remittance transaction is greater than or equal to the remittance amount; and if yes, each remittance transaction succeeds in the verification; and

if each remittance transaction succeeds in the verification, deducting the remittance amount in each remittance transaction from the balance of the remitter
20 account, and adding the remittance amount to a balance of the remittee account in each remittance transaction.

2. The method according to claim 1, wherein the verification on each remittance transaction further comprises determining whether the at least one reserved amount is
25 marked in a used state in the reserve fund list.

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

if the each remittance transaction succeeds in the verification, marking the reserved amount in the used state in the reserve fund list.

4. The method according to claim 1, wherein the reserve fund list further comprises
30 unique identifiers corresponding to the multiple reserved amounts, and each remittance transaction further comprises a unique identifier corresponding to the at least one reserved amount; and

the verification on each remittance transaction further comprises determining

whether the unique identifier has been used in a completed remittance transaction.

5. The method according to claim 1, wherein the balance of the remitter account, the balance of the remittee account, the reserved amounts, and the remittance amount undergo homomorphic encryption processing in advance;

5 the each remittance transaction further comprises a first zero knowledge proof generated based on the encrypted reserved amount and the encrypted remittance amount;

wherein determining whether the total reserved amount of the at least one reserved amount comprised in the remittance transaction is greater than or equal to the remittance amount comprises:

10 performing zero knowledge verification on the first zero knowledge proof based on a zero knowledge proof algorithm; and

the deducting the remittance amount in each remittance transaction from the balance of the remitter account, and adding the remittance amount to the balance of the remittee account in each remittance transaction comprises:

15 deducting the remittance amount from the balance of the remitter account through homomorphic encryption, and adding the remittance amount to the balance of the remittee account through homomorphic encryption.

6. The method according to claim 5, wherein the each remittance transaction further comprises a second zero knowledge proof generated based on the encrypted remittance amount; and

20 performing the verification of each remittance transaction further comprises performing zero knowledge verification on the second zero knowledge proof based on a zero knowledge proof algorithm to determine whether the remittance amount is greater than or equal to zero.

25 7. The method according to claim 1, further comprising:

receiving a second transaction that is sent by the remitter and that is used to initialize the reserve fund list, wherein the second transaction comprises the multiple reserved amounts obtained by dividing the balance of the remitter account;

30 determining whether a sum of the multiple reserved amounts comprised in the second transaction is less than or equal to the balance of the remitter account.

8. The method according to claim 7, wherein the balance of the remitter account and the multiple reserved amounts undergo homomorphic encryption processing in advance;

the second transaction further comprises a third zero knowledge proof generated

based on the multiple encrypted reserved amounts and the encrypted balance of the remitter account; and

performing zero knowledge verification on the third zero knowledge proof based on a zero knowledge proof algorithm to determine whether the sum of the multiple reserved amounts comprised in the second transaction is less than or equal to the balance of the remitter account.

9. The method according to claim 8, wherein the second transaction further comprises a fourth zero knowledge proof generated based on the multiple encrypted reserved amounts; and

performing zero knowledge verification on the fourth zero knowledge proof based on a zero knowledge proof algorithm to determine whether the multiple reserved amounts comprised in the second transaction each are greater than or equal to zero.

10. The method according to claim 7, further comprising:

marking each reserved amount comprised in the reserve fund list in an unused state.

11. The method according to claim 7, wherein the reserve fund list further comprises a unique identifier generated for each reserved amount.

12. The method according to claim 5, 6, 8, or 9, wherein the zero knowledge proof algorithm comprises a range proof algorithm.

13. A blockchain-based remittance apparatus, wherein a remitter account comprises a reserve fund list; and the reserve fund list comprises multiple reserved amounts obtained by dividing a balance of the remitter account; and

the apparatus comprises:

a receiving unit, configured to receive a plurality of remittance transactions, wherein each remittance transaction is sent by a remitter and is used for remittance to a remittee, wherein each remittance transaction comprises a remittance amount that is remitted by the remitter account to a remittee account and at least one reserved amount that corresponds to the remittance amount and that is allocated by the remitter from the reserve fund list to the remittance transaction, wherein at least one of the multiple reserved amounts is allocated to each remittance transaction in the plurality of remittance transactions;

a first transaction verification unit, configured to concurrently perform verification on the plurality of remittance transactions, wherein the first transaction verification unit comprises a first verification module, configured to determine whether a total reserved amount of the at least one reserved amount comprised in the remittance transaction is

greater than or equal to the remittance amount; and

an account update unit, configured to, if each remittance transaction succeeds in the verification, deduct the remittance amount in each remittance transaction from the balance of the remitter account, and add the remittance amount to a balance of the
5 remittee account in each remittance transaction.

14. The apparatus according to claim 13, wherein the first transaction verification unit further comprises a second verification module, configured to determine whether the at least one reserved amount is marked in a used state in the reserve fund list.

15. The apparatus according to claim 14, wherein the account update unit is further
10 configured to:

if the each remittance transaction succeeds in the verification, mark the reserved amount in the used state in the reserve fund list.

16. The apparatus according to claim 13, wherein the reserve fund list further comprises unique identifiers corresponding to the multiple reserved amounts, and each
15 remittance transaction further comprises a unique identifier corresponding to the at least one reserved amount; and

the first transaction verification unit further comprises a third verification module, configured to determine whether the unique identifier has been used in a completed remittance transaction.

20 17. The apparatus according to claim 13, wherein the balance of the remitter account, the balance of the remittee account, the reserved amounts, and the remittance amount undergo homomorphic encryption processing in advance;

the each remittance transaction further comprises a first zero knowledge proof generated based on the encrypted reserved amount and the encrypted remittance amount;

25 the first verification module is further configured to:

perform zero knowledge verification on the first zero knowledge proof based on a zero knowledge proof algorithm to determine whether the total reserved amount of the at least one reserved amount comprised in the remittance transaction is greater than or equal to the remittance amount; and

30 the account update unit is further configured to:

deduct the remittance amount in each remittance transaction from the balance of the remitter account through homomorphic encryption, and add the remittance amount to the balance of the remittee account in each remittance transaction through homomorphic encryption.

18. The apparatus according to claim 17, wherein the each remittance transaction further comprises a second zero knowledge proof generated based on the encrypted remittance amount; and

the first transaction verification unit further comprises a fourth verification module,
5 and the fourth verification module is configured to perform zero knowledge verification on the second zero knowledge proof based on a zero knowledge proof algorithm to determine whether the remittance amount is greater than or equal to zero.

19. The apparatus according to claim 13, wherein

the receiving unit is configured to receive a second transaction that is sent by the
10 remitter and that is used to initialize the reserve fund list, wherein the second transaction comprises the multiple reserved amounts obtained by dividing the balance of the remitter account;

the apparatus further comprises a second transaction verification unit, configured to perform second transaction verification on the second transaction, wherein the
15 second transaction verification unit comprises a fifth verification module, configured to determine whether a sum of the multiple reserved amounts comprised in the second transaction is less than or equal to the balance of the remitter account.

20. The apparatus according to claim 19, wherein the balance of the remitter account and the multiple reserved amounts undergo homomorphic encryption
20 processing in advance;

the second transaction further comprises a third zero knowledge proof generated based on the multiple encrypted reserved amounts and the encrypted balance of the remitter account; and

the fifth verification module is further configured to perform zero knowledge
25 verification on the third zero knowledge proof based on a zero knowledge proof algorithm to determine whether the sum of the multiple reserved amounts comprised in the second transaction is less than or equal to the balance of the remitter account.

21. The apparatus according to claim 20, wherein the second transaction further comprises a fourth zero knowledge proof generated based on the multiple encrypted
30 reserved amounts; and

the second transaction verification unit further comprises a sixth verification module, and the sixth verification module is configured to perform zero knowledge verification on the fourth zero knowledge proof based on a zero knowledge proof algorithm to determine whether the multiple reserved amounts comprised in the second

transaction each are greater than or equal to zero.

22. The apparatus according to claim 19, wherein the account update unit is further configured to:

mark each reserved amount comprised in the reserve fund list in an unused state.

5 23. The apparatus according to claim 19, wherein the reserve fund list further comprises a unique identifier generated for each reserved amount.

24. The apparatus according to claim 17, 18, 20, or 21, wherein the zero knowledge proof algorithm comprises a range proof algorithm.

25. A computer device, comprising a memory and a processor, wherein the
10 memory stores a computer program executable by the processor; and when executing the computer program, the processor performs the method according to any one of claims 1 to 12.

26. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program, and when executed by a processor, the computer
15 program performs the method according to any one of claims 1 to 12.