CLAIMS

What is claimed is:

1. A blockchain-based transaction method, comprising:

calculating a transaction amount commitment based on a commitment random number and a transaction amount involving a remitter account and a remitter account with respect to a blockchain;

obtaining a first commitment random number ciphertext and a first transaction amount ciphertext by encrypting the commitment random number and the transaction amount separately based on a homomorphic encryption public key of the remitter account using a homomorphic encryption algorithm;

obtaining a second commitment random number ciphertext and a second transaction amount ciphertext by encrypting the commitment random number and the transaction amount separately based on a homomorphic encryption public key of the remittee account using the homomorphic encryption algorithm; and

submitting transaction data to the blockchain, the transaction data including the transaction amount commitment, the first commitment random number ciphertext, the first transaction amount ciphertext, the second commitment random number ciphertext, and the second transaction amount ciphertext, for the transaction amount commitment, the first commitment random number ciphertext, and the first transaction amount ciphertext to be recorded into the remitter account, and the transaction amount commitment, the second commitment random number ciphertext, and the second transaction amount ciphertext to be recorded into the remittee account.

2. The method according to claim 1, wherein the remitter account registers a remitter balance commitment, a remitter random number ciphertext, and a remitter balance ciphertext in the blockchain; the remitter balance commitment is calculated based on a remitter random number and a remitter balance; the remitter random number ciphertext is calculated based on the remitter random number by using the homomorphic encryption algorithm; the remitter balance ciphertext is calculated based on the remitter balance by using the homomorphic encryption algorithm; and

wherein the remittee account registers a remittee balance commitment, a remittee

random number ciphertext, and a remittee balance ciphertext in the blockchain; the remittee balance commitment is calculated based on a remittee random number and a remittee balance; the remittee random number ciphertext is calculated based on the remittee random number by using the homomorphic encryption algorithm; the remittee balance ciphertext is calculated based on the remittee balance by using the homomorphic encryption algorithm.

3. The method according to claim 2, wherein the transaction amount commitment, the first transaction amount ciphertext, and the first commitment random number ciphertext are recorded into the remitter account by:

updating the remitter balance commitment based on the transaction amount commitment, updating the remitter random number ciphertext based on the first commitment random number ciphertext, and updating the remitter balance ciphertext based on the first transaction amount ciphertext; and

wherein the transaction amount commitment, the second transaction amount ciphertext, and the second commitment random number ciphertext are recorded into the remittee account by:

updating the remittee balance commitment based on the transaction amount commitment, updating the remittee random number ciphertext based on the second commitment random number ciphertext, and updating the remittee balance ciphertext based on the second transaction amount ciphertext.

4. The method according to claim 3, wherein an updated remitter balance commitment is a quotient of the remitter balance commitment and the transaction amount commitment; an updated remitter random number ciphertext is a quotient of the remitter random number ciphertext and the first commitment random number ciphertext; and an updated remitter balance ciphertext is a quotient of the remitter balance ciphertext and the first transaction amount ciphertext; and

wherein an updated remittee balance commitment is a product of the remittee balance commitment and the transaction amount commitment; an updated remittee random number ciphertext is a product of the remittee random number ciphertext and the second commitment random number ciphertext; and an updated remittee balance ciphertext is a product of the remittee balance ciphertext and the second transaction

amount ciphertext.

5. The method according to claim 1, wherein the obtaining the first commitment random number ciphertext and the first transaction amount ciphertext includes:

obtaining the first commitment random number ciphertext by encrypting the commitment random number based on a first encryption random number and the homomorphic encryption public key of the remitter account using the homomorphic encryption algorithm; and

obtaining the first transaction amount ciphertext by encrypting the transaction amount based on a second encryption random number and the homomorphic encryption public key of the remitter account using the homomorphic encryption algorithm.

6. The method according to claim 1, wherein the obtaining the second commitment random number ciphertext and the second transaction amount ciphertext includes:

obtaining the second commitment random number ciphertext by encrypting the commitment random number based on a third encryption random number and the homomorphic encryption public key of the remittee account using the homomorphic encryption algorithm; and

obtaining the second transaction amount ciphertext by encrypting the transaction amount based on a fourth encryption random number and the homomorphic encryption public key of the remittee account using the homomorphic encryption algorithm.

7. The method according to claim 1, comprising:

before the submitting the transaction data to the blockchain,

generating a first zero-knowledge proof, the first zero-knowledge proof configured to verify that the transaction amount is not less than 0;

wherein the transaction data includes the first zero-knowledge proof.

8. The method according to claim 1, comprising:

before the submitting the transaction data to the blockchain,

generating a second zero-knowledge proof, the second zero-knowledge proof configured to verify that the transaction amount is not greater than the remitter balance;

wherein the transaction data includes the second zero-knowledge proof.

9. The method according to claim 1, comprising:

before the submitting the transaction data to the blockchain,

generating a third zero-knowledge proof, the third zero-knowledge proof configured to verify that the commitment random number for calculating the transaction amount commitment is consistent with the commitment random number for calculating the second commitment random number ciphertext, and verify that the transaction amount for calculating the transaction amount commitment is consistent with the transaction amount for calculating the second transaction amount ciphertext;

wherein the transaction data includes the third zero-knowledge proof.

10. The method according to claim 1, comprising:

before the submitting the transaction data to the blockchain,

obtaining signature data by signing the transaction data using a signature private key of the remitter account;

wherein the transaction data includes the signature data.

11. The method according to claim 1, wherein the calculating the transaction amount commitment based on the commitment random number and the transaction amount includes:

obtaining a first transaction amount commitment based on a first commitment random number and the transaction amount, and obtaining a second transaction amount commitment based on a second commitment random number and the transaction amount;

wherein the obtaining the first commitment random number ciphertext and the first transaction amount ciphertext by encrypting the transaction amount includes:

obtaining the first transaction amount ciphertext and the first commitment random number ciphertext by encrypting the transaction amount and the first commitment random number separately based on the homomorphic encryption public key of the remitter account using the homomorphic encryption algorithm;

wherein the obtaining the second commitment random number ciphertext and the second transaction amount ciphertext by encrypting the commitment random number and the transaction amount separately based on the homomorphic encryption public key

of the remittee account using the homomorphic encryption algorithm includes:

obtaining the second commitment random number ciphertext and the second transaction amount ciphertext by encrypting the second commitment random number and the transaction amount separately based on the homomorphic encryption public key of the remittee account using the homomorphic encryption algorithm; and

wherein the transaction data includes the first transaction amount commitment, the second transaction amount commitment, the first transaction amount ciphertext, the first commitment random number ciphertext, the second transaction amount ciphertext, and the second commitment random number ciphertext, for the first transaction amount commitment, the first transaction amount ciphertext, and the first commitment random number ciphertext to be recorded into the remitter account, and the second transaction amount commitment, the second transaction amount ciphertext, and the second commitment random number ciphertext to be recorded into the remittee account.

12. The method according to claim 11, further comprising:

before the submitting the transaction data to the blockchain,

generating a fourth zero-knowledge proof, the fourth zero-knowledge proof configured to verify that the transaction amount for calculating the first transaction amount commitment is consistent with the transaction amount for calculating the second transaction amount commitment;

wherein the transaction data further includes the fourth zero-knowledge proof.

13. A blockchain-based transaction apparatus, comprising:

a calculation unit, configured to calculate a transaction amount commitment based on a commitment random number and a transaction amount involving a remitter account and a remittee account with respect to a blockchain;

a first encryption unit, configured to obtain a first commitment random number ciphertext and a first transaction amount ciphertext by encrypting the commitment random number and the transaction amount separately based on a homomorphic encryption public key of the remitter account using a homomorphic encryption algorithm;

a second encryption unit, configured to obtain a second commitment random number ciphertext and a second transaction amount ciphertext by encrypting the

commitment random number and the transaction amount separately based on a homomorphic encryption public key of the remittee account using the homomorphic encryption algorithm; and

a submission unit, configured to submit transaction data to the blockchain, the transaction data including the transaction amount commitment, the first commitment random number ciphertext, the first transaction amount ciphertext, the second commitment random number ciphertext, and the second transaction amount ciphertext, for the transaction amount commitment, the first commitment random number ciphertext, and the first transaction amount ciphertext to be recorded into the remitter account, and the transaction amount commitment, the second commitment random number ciphertext, and the second transaction amount ciphertext to be recorded into the remittee account.

14. A system, comprising:

a memory, configured to store computer instructions; and

a processor, configured to execute the computer instructions to implement acts including:

calculating a transaction amount commitment based on a commitment random number and a transaction amount involving a remitter account and a remitter account with respect to a blockchain;

obtaining a first commitment random number ciphertext and a first transaction amount ciphertext by encrypting the commitment random number and the transaction amount separately based on a homomorphic encryption public key of the remitter account using a homomorphic encryption algorithm;

obtaining a second commitment random number ciphertext and a second transaction amount ciphertext by encrypting the commitment random number and the transaction amount separately based on a homomorphic encryption public key of the remittee account using the homomorphic encryption algorithm; and

submitting transaction data to the blockchain, the transaction data including the transaction amount commitment, the first commitment random number ciphertext, the first transaction amount ciphertext, the second commitment random number ciphertext, and the second transaction amount ciphertext, for the transaction amount commitment, the first commitment random number ciphertext, and the first transaction amount

ciphertext to be recorded into the remitter account, and the transaction amount commitment, the second commitment random number ciphertext, and the second transaction amount ciphertext to be recorded into the remittee account.

15. The system according to claim 14, wherein the remitter account registers a remitter balance commitment, a remitter random number ciphertext, and a remitter balance ciphertext in the blockchain; the remitter balance commitment is calculated based on a remitter random number and a remitter balance; the remitter random number ciphertext is calculated based on the remitter random number by using the homomorphic encryption algorithm; the remitter balance ciphertext is calculated based on the remitter balance by using the homomorphic encryption algorithm; and

wherein the remittee account registers a remittee balance commitment, a remittee random number ciphertext, and a remittee balance ciphertext in the blockchain; the remittee balance commitment is calculated based on a remittee random number and a remittee balance; the remittee random number ciphertext is calculated based on the remittee random number by using the homomorphic encryption algorithm; the remittee balance ciphertext is calculated based on the remittee balance by using the homomorphic encryption algorithm.

16. The system according to claim 15, wherein the transaction amount commitment, the first transaction amount ciphertext, and the first commitment random number ciphertext are recorded into the remitter account by:

updating the remitter balance commitment based on the transaction amount commitment, updating the remitter random number ciphertext based on the first commitment random number ciphertext, and updating the remitter balance ciphertext based on the first transaction amount ciphertext; and

wherein the transaction amount commitment, the second transaction amount ciphertext, and the second commitment random number ciphertext are recorded into the remittee account by:

updating the remittee balance commitment based on the transaction amount commitment, updating the remittee random number ciphertext based on the second commitment random number ciphertext, and updating the remittee balance ciphertext based on the second transaction amount ciphertext.

17. The system according to claim 16, wherein an updated remitter balance commitment is a quotient of the remitter balance commitment and the transaction amount commitment; an updated remitter random number ciphertext is a quotient of the remitter random number ciphertext and the first commitment random number ciphertext; and an updated remitter balance ciphertext is a quotient of the remitter balance ciphertext and the first transaction amount ciphertext; and

wherein an updated remittee balance commitment is a product of the remittee balance commitment and the transaction amount commitment; an updated remittee random number ciphertext is a product of the remittee random number ciphertext and the second commitment random number ciphertext; and an updated remittee balance ciphertext is a product of the remittee balance ciphertext and the second transaction amount ciphertext.

18. The system according to claim 14, wherein the obtaining the first commitment random number ciphertext and the first transaction amount ciphertext includes:

obtaining the first commitment random number ciphertext by encrypting the commitment random number based on a first encryption random number and the homomorphic encryption public key of the remitter account using the homomorphic encryption algorithm; and

obtaining the first transaction amount ciphertext by encrypting the transaction amount based on a second encryption random number and the homomorphic encryption public key of the remitter account using the homomorphic encryption algorithm.

19. The system according to claim 14, wherein the obtaining the second commitment random number ciphertext and the second transaction amount ciphertext includes:

obtaining the second commitment random number ciphertext by encrypting the commitment random number based on a third encryption random number and the homomorphic encryption public key of the remittee account using the homomorphic encryption algorithm; and

obtaining the second transaction amount ciphertext by encrypting the transaction amount based on a fourth encryption random number and the homomorphic encryption

public key of the remittee account using the homomorphic encryption algorithm.

20. The system according to claim 14, wherein the calculating the transaction amount commitment based on the commitment random number and the transaction amount includes:

obtaining a first transaction amount commitment based on a first commitment random number and the transaction amount, and obtaining a second transaction amount commitment based on a second commitment random number and the transaction amount;

wherein the obtaining the first commitment random number ciphertext and the first transaction amount ciphertext by encrypting the transaction amount includes:

obtaining the first transaction amount ciphertext and the first commitment random number ciphertext by encrypting the transaction amount and the first commitment random number separately based on the homomorphic encryption public key of the remitter account using the homomorphic encryption algorithm;

wherein the obtaining the second commitment random number ciphertext and the second transaction amount ciphertext by encrypting the commitment random number and the transaction amount separately based on the homomorphic encryption public key of the remittee account using the homomorphic encryption algorithm includes:

obtaining the second commitment random number ciphertext and the second transaction amount ciphertext by encrypting the second commitment random number and the transaction amount separately based on the homomorphic encryption public key of the remittee account using the homomorphic encryption algorithm; and

wherein the transaction data includes the first transaction amount commitment, the second transaction amount commitment, the first transaction amount ciphertext, the first commitment random number ciphertext, the second transaction amount ciphertext, and the second commitment random number ciphertext, for the first transaction amount commitment, the first transaction amount ciphertext, and the first commitment random number ciphertext to be recorded into the remitter account, and the second transaction amount commitment, the second transaction amount ciphertext, and the second commitment random number ciphertext to be recorded into the remittee account.