

Claims

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 remittee account with respect to a blockchain;

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

obtaining a second commitment random number ciphertext by encrypting the commitment random number based on a homomorphic encryption public key of the remittee account and the transaction amount 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, and the second commitment random number ciphertext, for the transaction amount commitment and the first commitment random number ciphertext to be recorded into the remitter account, and the transaction amount commitment and the second commitment random number ciphertext to be recorded into the remittee account.

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

wherein the remittee account registers a remittee balance commitment and a remittee random number 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 obtained by encrypting the remittee random number based on the remittee balance by using the homomorphic encryption algorithm.

3. The method according to claim 2, wherein the transaction amount commitment 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, and updating the remitter random number ciphertext based on the first commitment random number ciphertext; and

wherein the transaction amount commitment 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, and updating the remittee random number ciphertext based on the second commitment random number 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; and the updated remitter random number ciphertext is a quotient of the remitter random number ciphertext and the first commitment random number ciphertext; and

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

5. 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.

6. 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.

7. 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, the commitment random number for calculating the first commitment random number ciphertext, and the commitment random number for calculating the second commitment random number ciphertext are consistent with one another, and to verify that the transaction amount for calculating the transaction amount commitment, the transaction amount for calculating the first commitment random number ciphertext, and the transaction amount for calculating the second commitment random number ciphertext are consistent with one another; wherein the transaction data includes the third zero-knowledge proof.

8. The method according to claim 1, comprising:

before the submitting the transaction data to the blockchain,

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

wherein the transaction data includes the signature data.

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

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

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

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

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

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

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

10. The method according to claim 9, 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 a first transaction amount for calculating the first transaction amount commitment and a second transaction amount for calculating the second transaction amount commitment are consistent with one another;

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

11. 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 by encrypting the commitment random number based on a homomorphic encryption public key of the remitter account and the transaction amount using a homomorphic encryption algorithm;

a second encryption unit, configured to obtain a second commitment random number ciphertext by encrypting the commitment random number based on a homomorphic encryption public key of the remittee account and the transaction amount 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, and the second commitment random number ciphertext, for the transaction amount commitment and the first commitment random number ciphertext to be recorded into the remitter account, and the transaction amount commitment and the second commitment random number ciphertext to be recorded into the remittee account.

12. A remitter device, 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 remittee account with respect to a blockchain;

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

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

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

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

13. The device according to claim 12, wherein the remitter account registers a remitter balance commitment and a remitter random number 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 obtained by encrypting the remitter random number based on the remitter balance by using the homomorphic encryption algorithm; and

wherein the remittee account registers a remittee balance commitment and a remittee random number 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 obtained by encrypting the remittee random number based on the remittee balance by using the homomorphic encryption algorithm.

14. The device according to claim 13, wherein the transaction amount commitment 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, and updating the remitter random number ciphertext based on the first commitment random number ciphertext; and

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

15. The device according to claim 14, wherein an updated remitter balance commitment is a quotient of the remitter balance commitment and the transaction amount

commitment; and the updated remitter random number ciphertext is a quotient of the remitter random number ciphertext and the first commitment random number ciphertext; and

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

16. The device according to claim 12, wherein the acts includes:
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.

17. The device according to claim 12, 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.

18. The device according to claim 12, wherein the acts include:
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, the commitment random number for calculating the first commitment random
number ciphertext, and the commitment random number for calculating the second commitment
random number ciphertext are consistent with one another, and to verify that the transaction
amount for calculating the transaction amount commitment, the transaction amount for
calculating the first commitment random number ciphertext, and the transaction amount for
calculating the second commitment random number ciphertext are consistent with one another;
wherein the transaction data includes the third zero-knowledge proof.

19. The device according to claim 12, wherein the acts include:
before the submitting the transaction data to the blockchain,
obtaining a signature data by signing the transaction data using a signature private key of the remitter account;
wherein the transaction data includes the signature data.

20. The device according to claim 12, wherein the calculating the transaction amount commitment based on the commitment random number and the transaction amount includes:

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

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

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

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

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

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

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