

Method, Apparatus and Electronic Device for Blockchain Transactions

CROSS REFERENCE TO RELATED APPLICATION

[0001] The present application is based on and claims priority to Chinese Patent Application No. 201810886845.3, filed on August 6, 2018, which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] One or more embodiments of the present specification relate to the technical field of blockchain, particularly to a method, apparatus, and electronic device for implementing blockchain-based transactions.

BACKGROUND

[0003] Blockchain nodes of a blockchain network may jointly maintain a unified blockchain ledger through a consensus reached among the blockchain nodes, to record data of transactions having occurred on the blockchain network. The blockchain ledger can be made public for viewing and verification of historical data of the occurred transactions at any time.

SUMMARY

[0004] One or more embodiments of the present specification provide a method, apparatus, and non-transitory computer-readable storage medium for implementing blockchain-based transactions.

[0005] According to a first aspect of one or more embodiments of the present specification, a method for implementing blockchain-based transactions is provided. The method may comprise: determining a transaction amount to be remitted from a remitter's blockchain account into a receiver's blockchain account, wherein a commitment of the remitter's balance is recorded with the remitter's blockchain account in a blockchain, a commitment of the receiver's balance is recorded with the receiver's blockchain account in the blockchain, the commitment of the remitter's balance is calculated by using a homomorphic encryption algorithm according to the remitter's balance, and the commitment of the receiver's balance is calculated by using the homomorphic encryption algorithm according to the receiver's balance; obtaining a commitment of the transaction amount by using the homomorphic encryption algorithm according to the transaction amount; and submitting to the blockchain a

transaction comprising information of the remitter's blockchain account, information of the receiver's blockchain account, and the commitment of the transaction amount, for the commitment of the transaction amount to be deducted from the commitment of the remitter's balance and the commitment of the transaction amount to be added to the commitment of the receiver's balance after the transaction is implemented by the blockchain.

[0006] In some embodiments, the commitment of the receiver's balance is calculated by using the homomorphic encryption algorithm according to the receiver's balance and a first random number; the commitment of the transaction amount is calculated by using the homomorphic encryption algorithm according to the transaction amount and a transaction random number; the computing device is associated with the remitter; before submitting the transaction, the method further comprises sending the transaction random number to another computing device associated with the receiver via an off-chain channel for the computing device associated with the receiver to determine an updated receiver's balance according to an updated commitment of the receiver's balance and an updated first random number; the updated commitment of the receiver's balance is a sum of the commitment of the transaction amount and the commitment of the receiver's balance; the updated first random number is a sum of the transaction random number and the first random number; and the updated receiver's balance is a sum of the receiver's balance and the transaction amount.

[0007] In some embodiments, before submitting the transaction, the method may further comprise: sending the commitment of the transaction amount to the computing device associated with the receiver via the off-chain channel for the computing device associated with the receiver to verify an association among the commitment of the transaction amount, the transaction random number, and the transaction amount.

[0008] In some embodiments, before submitting the transaction, the method may further comprise: obtaining a receiver signature generated by the computing device associated with the receiver based on a receiver private key and related to the commitment of the transaction amount, wherein the receiver signature is generated after the association has been verified; and adding the receiver signature to the transaction for the blockchain nodes in the blockchain to verify the receiver signature.

[0009] In some embodiments, before submitting the transaction, the method may further comprise: generating a remitter signature related to the commitment of the transaction amount based on a remitter private key; and adding the remitter signature to the transaction

for the blockchain nodes in the blockchain to verify the remitter signature.

[0010] In some embodiments, the commitment of the remitter's balance is calculated by using the homomorphic encryption algorithm according to the remitter's balance and a second random number; the commitment of the transaction amount is calculated by using the homomorphic encryption algorithm according to the transaction amount and a transaction random number; for the blockchain to implement the transaction, the transaction amount is deducted from the remitter's balance; and the transaction random number is deducted from the second random number after the transaction is implemented.

[0011] In some embodiments, before submitting the transaction, the method may further comprise: generating a range proof according to the second random number, the remitter's balance, the commitment of the remitter's balance, the transaction random number, the transaction amount, and the commitment of the transaction amount; and adding the range proof to the transaction for the blockchain nodes in the blockchain to verify whether the transaction amount is not less than zero and not more than the remitter's balance.

[0012] According to a second aspect of one or more embodiments of the present specification, an apparatus for implementing blockchain-based transactions is provided. The apparatus may comprise: one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the system to perform operations comprising: determining a transaction amount to be remitted from a remitter's blockchain account into a receiver's blockchain account, wherein a commitment of the remitter's balance is recorded with the remitter's blockchain account in a blockchain, a commitment of the receiver's balance is recorded with the receiver's blockchain account in the blockchain, the commitment of the remitter's balance is calculated by using a homomorphic encryption algorithm according to the remitter's balance, and the commitment of the receiver's balance is calculated by using the homomorphic encryption algorithm according to the receiver's balance; obtaining a commitment of the transaction amount by using the homomorphic encryption algorithm according to the transaction amount; and submitting to the blockchain a transaction comprising information of the remitter's blockchain account, information of the receiver's blockchain account, and the commitment of the transaction amount, for the commitment of the transaction amount to be deducted from the commitment of the remitter's balance and the commitment of the transaction amount to

be added to the commitment of the receiver's balance after the transaction is implemented by the blockchain.

[0013] According to a third aspect of one or more embodiments of the present specification, a non-transitory computer-readable storage medium is provided. The non-transitory computer-readable storage medium may be configured with instructions executable by one or more processors to cause the one or more processors to perform operations comprising: determining a transaction amount to be remitted from a remitter's blockchain account into a receiver's blockchain account, wherein a commitment of the remitter's balance is recorded with the remitter's blockchain account in a blockchain, a commitment of the receiver's balance is recorded with the receiver's blockchain account in the blockchain, the commitment of the remitter's balance is calculated by using a homomorphic encryption algorithm according to the remitter's balance, and the commitment of the receiver's balance is calculated by using the homomorphic encryption algorithm according to the receiver's balance; obtaining a commitment of the transaction amount by using the homomorphic encryption algorithm according to the transaction amount; and submitting to the blockchain a transaction comprising information of the remitter's blockchain account, information of the receiver's blockchain account, and the commitment of the transaction amount, for the commitment of the transaction amount to be deducted from the commitment of the remitter's balance and the commitment of the transaction amount to be added to the commitment of the receiver's balance after the transaction is implemented by the blockchain.

BRIEF DESCRIPTION OF THE DRAWING

[0014] FIG. 1 is a flow chart of a method for implementing blockchain-based transactions according to some embodiments of the specification.

[0015] FIG. 2 is a schematic diagram of an implementation of a remittance transaction in a blockchain network according to some embodiments of the specification.

[0016] FIG. 3 is a flow chart of an implementation of a remittance transaction in a blockchain network according to some embodiments of the specification.

[0017] FIG. 4 is a structure diagram of a device for implementing blockchain-based transactions according to some embodiments of the specification.

[0018] FIG. 5 is a block diagram of an apparatus for implementing blockchain-based transactions according to some embodiments of the specification.

DETAILED DESCRIPTION

[0019] Embodiments will be described in detail, with examples shown in the accompanying drawings. When the description below involves the accompanying drawings, unless otherwise indicated, the same numeral in different accompanying drawings stands for the same element or similar elements. The implementation manners described in the following embodiments do not represent all the implementation manners consistent with the present specification. Rather, they are only examples of the apparatuses and methods described in detail in the attached claims and consistent with some aspects of one or more embodiments of the present specification.

[0020] In some embodiments, it is not necessary to perform steps in the methods according to the sequence illustrated and described in the present specification. In some other embodiments, the steps of the methods may be more or less than those described in the present specification. Further, a single step described in the present specification may be split into multiple steps for description in other embodiments, while multiple steps described in the present specification may be merged into one single step for description in yet other embodiments.

[0021] FIG. 1 is a flow chart of a method for implementing blockchain-based transactions according to some embodiments of the specification. As shown in FIG. 1, this method is implementable by one or more computing devices as one or more remitter devices and may comprise the following steps 102-106.

[0022] Step 102, determining a transaction amount to be remitted from a remitter's blockchain account into a receiver's blockchain account, wherein a commitment of the remitter's balance is recorded with the remitter's blockchain account in a blockchain, a commitment of the receiver's balance is recorded with the receiver's blockchain account in the blockchain, the commitment of the remitter's balance is calculated by using a homomorphic encryption algorithm according to the remitter's balance, and the commitment of the receiver's balance is calculated by using the homomorphic encryption algorithm according to the receiver's balance.

[0023] In some embodiments, the remitter's balance refers to a balance of the remitter's blockchain account in the blockchain. Similarly, the receiver's balance refers to a balance of the receiver's blockchain account in the blockchain. Therefore, a balance of an account may

also be referred to as an account balance hereinafter.

[0024] In some embodiments, a remitter user may negotiate with a receiver user to determine a transaction amount. A remitter user may be associated with a remitter device (e.g., a computing device associated with the remitter user), and a receiver user may be associated with a receiver device (a computing device associated with the receiver user). The computing device may be a personal computer, a laptop computer, a cell phone, a camera phone, a smart phone, a PDA (personal digital assistant), a media player, a navigation device, an email sending and receiving device, a game console, a tablet computer, a wearable device or any combination of a few of these devices. A blockchain-based transaction between the remitter device and the receiver devices can be performed by remitting (or transferring) an asset certificate corresponding to the transaction amount from a remitter blockchain account to a receiver blockchain account. The asset certificate may correspond to a token, a digital asset, or any other intelligent asset in a blockchain. Alternatively, the asset certificate may also correspond to cash, security, a discount coupon, a real estate, and any other off-chain asset. This is not limited by embodiments of the present specification.

[0025] In some embodiments, the blockchain nodes in a blockchain may respectively maintain unified blockchain ledgers based on a consensus, so by registering the commitment of the remitter's balance and the commitment of the receiver's balance in the blockchain, the blockchain ledgers maintained by the blockchain nodes may record the commitment of the remitter's balance and the commitment of the receiver's balance, and may not record the remitter's balance and the receiver's balance. As a result, the balance held by the remitter user and the balance held by the receiver user are concealed from the public as private data.

[0026] Step 104, obtaining a commitment of the transaction amount by using the homomorphic encryption algorithm according to the transaction amount.

[0027] In some embodiments, the commitment of the transaction amount can be calculated based on the transaction amount by using the homomorphic encryption algorithm. In some embodiments, any type of homomorphic encryption algorithm may be adopted. For example, any homomorphic encryption algorithm satisfying additive homomorphism and supporting proof that plaintext data belongs to a range may be used. The homomorphic encryption algorithm may allow the commitment of the transaction amount to be deducted from the commitment of the remitter's balance and the commitment of the transaction amount to be added to the commitment of the receiver's balance, and allow the remitter to provide a proof

that the transaction amount is not less than zero and not more than the remitter's account balance. The present specification has no limitation on whether the homomorphic encryption algorithm is an additively homomorphic encryption algorithm or a fully homomorphic encryption algorithm.

[0028] In some embodiments, the homomorphic encryption algorithm may generate a random number, so that corresponding commitment data can be calculated based on the random number and unencrypted data. The random number can be used to decrypt the commitment data to obtain unencrypted data, or to verify whether the commitment data corresponds to the unencrypted data. For example, the homomorphic encryption algorithm may be a Pedersen commitment mechanism.

[0029] In some embodiments, the commitment of the receiver's balance is calculated by using the homomorphic encryption algorithm according to the receiver's balance and a receiver random number. The commitment of the transaction amount is calculated by using the homomorphic encryption algorithm according to the transaction amount and a transaction random number. Accordingly, a remitter device may send the transaction random number to the receiver device via an off-chain channel so that the receiver device determines an updated receiver's balance according to an updated commitment of the receiver's balance and an updated receiver random number. The updated commitment of the receiver's balance is obtained by adding the commitment of the transaction amount to the commitment of the receiver's balance. The updated receiver random number is obtained by adding the transaction random number to the receiver random number. The updated receiver's balance is the sum of the receiver's balance and the transaction amount. In some embodiments, a receiver random number may refer to a random number used for generating the commitment of the receiver's balance based on the homomorphic encryption algorithm. Similarly, a transaction random number may refer to a random number used for generating the commitment of the transaction amount based on the homomorphic encryption algorithm.

[0030] In some embodiments, a remitter device may send the commitment of the transaction amount to a receiver device via an off-chain channel before submitting the transaction so that the receiver device verifies the association among the commitment of the transaction amount, the transaction random number, and the transaction amount. A receiver device may allow the implementation of the transaction after successful verification, otherwise may stop the implementation of the transaction. For example, a receiver device may provide a receiver

signature after successful verification, and otherwise may not provide this receiver signature.

[0031] In some embodiments, a remitter device may obtain a receiver signature generated by a receiver device based on a receiver private key and is related to the commitment of a transaction amount. The receiver signature is generated by the receiver device after the above-described associations have been verified, and then added to the transaction so that the blockchain nodes in the blockchain can conduct signature verification to verify the receiver signature. For example, when a transaction does not contain the receiver signature, the blockchain nodes may determine that consensus fails, thereby refusing to proceed with the transaction.

[0032] In some embodiments, the commitment of the remitter's balance may be calculated by using the homomorphic encryption algorithm according to the remitter's balance and a remitter random number, and the commitment of the transaction amount may be calculated by using the homomorphic encryption algorithm according to the transaction amount and a transaction random number. The transaction amount is deducted from the remitter's balance and the transaction random number is deducted from the remitter random number after the transaction is implemented. Subsequent transactions may be executed based on the updated remitter's balance obtained after the transaction amount is deducted and the updated remitter random number obtained after the transaction random number is deducted. In some embodiments, a remitter random number may refer to a random number used for generating the commitment of the remitter's balance.

[0033] In some embodiments, a remitter device may generate a range proof according to the remitter random number, the remitter's balance, the commitment of the remitter's balance, the transaction random number, the transaction amount, and the commitment of the transaction amount, and add the range proof to the transaction so that the blockchain nodes in the blockchain can verify whether the transaction amount is not less than zero and not more than the remitter's balance. For instance, range proof technologies such as a Bulletproofs solution or a Borromean ring signature solution may be used.

[0034] In some embodiments, a remitter device may generate a remitter signature related to the commitment of a transaction amount via a remitter private key, and add the remitter signature to the transaction so that the blockchain nodes in the blockchain can conduct signature verification to verify the remitter signature. For example, when a transaction does not contain a remitter signature, the blockchain nodes may determine that consensus fails,

and may not proceed with the transaction. In other embodiments, the remitter signature may further be related to a range proof.

[0035] Step 106, submitting to the blockchain a transaction comprising information of the remitter's blockchain account, information of the receiver's blockchain account, and the commitment of the transaction amount, for the commitment of the transaction amount to be deducted from the commitment of the remitter's balance and the commitment of the transaction amount to be added to the commitment of the receiver's balance after the transaction is implemented by the blockchain.

[0036] In some embodiments, a commitment of the transaction amount is used in a transaction, so that the blockchain ledgers may record the commitment of the transaction amount, instead of the underlying transaction amount, thereby concealing and keeping confidential the value of the transaction amount. In addition, a commitment of the remitter's balance, a commitment of the receiver's balance, and a commitment of the transaction amount are generated by using a homomorphic encryption algorithm. As a result, even without acquiring the remitter's balance, the receiver's balance, and the transaction amount, the transaction can be carried out, as deduction operations can be performed between the commitment of the remitter's balance and the commitment of the transaction amount, and addition operations can be performed between the commitment of the receiver's balance and the commitment of the transaction amount. Thus, the transaction can be implemented smoothly without disclosing private data.

[0037] In some embodiments, after blockchain nodes receive the foregoing transaction, the blockchain nodes may use double-spending prevention mechanism or replay attack prevention mechanism to verify if this transaction has been executed. If this transaction has been executed, another execution of this transaction may be rejected.

[0038] For easier understanding, a remittance transaction in a blockchain network is taken below as an example to describe the technical solutions of the present specification in detail. FIG. 2 is a schematic diagram of implementation of a remittance transaction in a blockchain network according to some embodiments of the specification. As shown in FIG. 2, it is assumed that a user A conducts blockchain remittance to a user B. A "user" in the present specification may be manifested as a logged-in user account, while this user account may belong to an individual or an organization.

[0039] It is assumed that a remitter device used by the user A is a user device 1. For instance, a user account corresponding to the user A is logged in on this user device 1. Similarly, a receiver device used by the user B is a user device 2. An off-chain channel may be established between the user device 1 and the user device 2 to achieve corresponding off-chain communications.

[0040] A client program of blockchain may be run on the user device 1 so that the user device 1 communicates with a corresponding blockchain node in the blockchain network, such as the node 1 shown in FIG. 2. Similarly, a client program of blockchain may be run on the user device 2 so that the user device 2 also communicates with a corresponding blockchain node in the blockchain network, such as the node 2 shown in FIG. 2. The blockchain network also includes other blockchain nodes, such as the node i shown in FIG. 2. The blockchain nodes are not enumerated here. Through the foregoing node 1, node 2, etc., the remittance transaction between the user A and the user B may be implemented via the blockchain network, and related transaction information may be recorded in the blockchain ledgers maintained by the blockchain nodes respectively, thereby preventing the recorded transaction information from being tampered with, and also facilitating subsequent inspection.

[0041] With respect to the scenario of the remittance transaction shown in FIG. 2, FIG. 3 is a flow chart of implementation of a remittance transaction in a blockchain network according to some embodiments of the specification. As shown in FIG. 3, the process of interaction among the remitter, receiver, and blockchain nodes may comprise the following steps 301-311.

[0042] Step 301, the remitter drafts a remittance transaction.

[0043] In some embodiments, a remitter may refer to an individual or entity that remits a fund or other resources in a remittance transaction; correspondingly, a receiver may refer to an individual or entity that receives a fund or other resources in the remittance transaction. For example, in the embodiments shown in FIG. 2, the user device 1 may be configured to be the remitter, while the user device 2 may be configured to be the receiver.

[0044] In some embodiments, when drafting a remittance transaction, a remitter may negotiate a remittance amount t with a receiver. The remitter may apply homomorphic encryption to the remittance amount t based on a Pedersen commitment mechanism. The

remitter may generate a remittance random number r for the remittance amount t , and the remittance commitment corresponding to the remittance amount t is $T = \text{Comm}(r, t) = g^r h^t$, where, g and h are known parameters in the algorithm.

[0045] Step 302, the remitter sends (r, t, T) to a receiver via an off-chain channel.

[0046] In some embodiments, sending (r, t, T) via an off-chain channel rather than a blockchain network may avoid recording the remittance random number r and the remittance amount t in a blockchain ledger, and ensure that the remittance amount t is unknown except to the remitter and the receiver.

[0047] Step 303, the receiver verifies the received (r, t, T) .

[0048] In some embodiments, the receiver may verify the remittance amount t to determine that it is the negotiated remittance amount. In some embodiments, if the remittance amount t is correct, the receiver may verify the remittance commitment T ; in other words, the receiver may calculate the remittance random number r and the remittance amount t via the encryption algorithm based on a Pedersen commitment mechanism to verify if the remittance commitment $T = \text{Comm}(r, t)$ is correct. If yes, the verification is passed. If no, the verification is not passed.

[0049] Step 304, after the verification is passed, a receiver signature is generated and returned to the remitter.

[0050] In some embodiments, after the verification is passed, the receiver may use a receiver private key to sign (A, B, T) , generate a signature SIGB , and return the signature to the remitter. This signature SIGB indicates that the receiver agrees that the remittance transaction with a commitment T is to be implemented from the blockchain account 1 of the user A to the blockchain account 2 of user B.

[0051] Step 305, after receiving the signature SIGB , the remitter generates a range proof PR .

[0052] In some embodiments, after the remitter receives the signature SIGB , the remitter determines that the receiver allows implementation of the remittance transaction. The remitter conducts the remittance transaction to the receiver. The remittance operation from the blockchain account 1 corresponding to the user A to the blockchain account 2 corresponding to the user B may be executed. In some embodiments, the balance s_A in the blockchain

account 1 and the balance s_B in the blockchain account 2 may be recorded in the blockchain ledgers maintained by various blockchain nodes. In other embodiments, instead of directly recording the balances, a balance commitment S_A corresponding to the account balance s_A and a balance commitment S_B corresponding to the account balance s_B may be recorded for privacy protection. The balance commitment $S_A = \text{Comm}(r_A, s_A)$, the balance commitment $S_B = \text{Comm}(r_B, s_B)$, r_A is a random number corresponding to s_A , and r_B is a random number corresponding to s_B .

[0053] In some embodiments, to ensure a smooth completion of the remittance transaction, blockchain nodes may determine that the values of the remittance amount t and the account balance s_A meet the following conditions: $t \geq 0$ and $s_A - t \geq 0$; while range proof technologies enable the blockchain nodes to verify whether the transaction meets the predetermined conditions. For example, the Bulletproofs solution or the Borromean ring signature solution may be used to achieve this. Other solutions may also be used. The remitter may use a range proof technology to generate a corresponding range proof PR related to (r_A, s_A, S_A, r, t, T) so as to enable the blockchain nodes to verify if the conditions of $t \geq 0$ and $s_A - t \geq 0$ are met in the subsequent process.

[0054] Step 306, the remitter signs the transaction $(A, B, T; PR)$ to generate a signature $SIGA$.

[0055] In some embodiments, the remitter may generate the signature $SIGA$ by signing the transaction $(A, B, T; PR)$ based on a remitter private key.

[0056] Step 307, the remitter submits the transaction to the blockchain.

[0057] In some embodiments, the remitter may submit the corresponding remittance transaction $(A, B, T; PR; SIGA, SIGB)$ to the blockchain via a node 1 to execute this remittance transaction. The remittance transaction $(A, B, T; PR; SIGA, SIGB)$ may be transmitted to all the blockchain nodes in the blockchain network and all the blockchain nodes may verify this remittance transaction $(A, B, T; PR; SIGA, SIGB)$ respectively and execute a remittance operation when the verification is passed, or to reject the remittance when the verification is not passed.

[0058] Step 308, the blockchain nodes check if the transaction has been executed.

[0059] In some embodiments, every blockchain node in the blockchain network may receive the remittance transaction $(A, B, T; PR; SIGA, SIGB)$, and perform verification and

other operations through Steps 308-311.

[0060] In some embodiments, after the blockchain nodes receive the remittance transaction (A, B, T; PR; SIGA, SIGB), the blockchain nodes may use the double-spending prevention mechanism or replay attack prevention mechanism to verify if this remittance transaction has been executed. If this remittance transaction has been executed, another execution of this remittance transaction (A, B, T; PR; SIGA, SIGB) may be rejected, otherwise the process proceeds to Step 309.

[0061] Step 309, the blockchain nodes check the signatures.

[0062] In some embodiments, the blockchain nodes may check if the signatures SIGA and SIGB contained in the remittance transaction (A, B, T; PR; SIGA, SIGB) are correct. If any of the signatures is not correct, the execution of this remittance transaction (A, B, T; PR; SIGA, SIGB) may be rejected, otherwise the process proceeds to Step 310.

[0063] Step 310, the blockchain nodes check the range proof PR.

[0064] In some embodiments, the blockchain nodes may, based on a range proof technology, check the range proof PR contained in the remittance transaction (A, B, T; PR; SIGA, SIGB) to determine if the conditions of $t \geq 0$ and $s_A - t \geq 0$ are met. If the conditions are not met, the execution of this remittance transaction (A, B, T; PR; SIGA, SIGB) may be rejected, otherwise the process proceeds to Step 311.

[0065] Step 311, in the maintained blockchain ledgers, the blockchain nodes update the balances in the blockchain accounts of the user A and the user B.

[0066] In some embodiments, after the verification in Steps 308 - 310 is passed, the blockchain nodes may deduct the remittance commitment T from the balance commitment S_A corresponding to the account balance s_A recorded in the blockchain ledgers, and add the remittance commitment T to the balance commitment S_B corresponding to the account balance s_B , so that the balance commitment in the blockchain account 1 corresponding to the user A is updated to $S_A - T$, and the balance commitment in the blockchain account 2 corresponding to the user B is updated to $S_B + T$.

[0067] Based on the properties of the homomorphic encryption algorithm, the updated balance commitment $S_A - T$ follows $S_A - T = \text{Comm}(r_A - r, s_A - t)$, because the balance commitment $S_A = \text{Comm}(r_A, s_A)$ and $T = \text{Comm}(r, t)$. The user device 1 knows $r_A - r$ and can acquire $S_A - T$

from the blockchain ledger maintained by the node 1, and s_{A-t} can then be determined. Similarly, the updated balance commitment S_{B+T} follows $S_{B+T} = \text{Comm}(r_B + r, s_B + t)$, because the balance commitment $S_B = \text{Comm}(r_B, s_B)$ and $T = \text{Comm}(r, t)$. The user device 2 knows r_B , has been notified of the transaction random number r by the remitter in Step 302, and can acquire S_{B+T} from the blockchain ledger maintained by the node 2, and $s_B + t$ can then be determined.

[0068] To sum up, the use of the homomorphic encryption mechanism allows the encryption of the balances in blockchain accounts. After encryption, the balance commitments can be recorded in blockchain ledgers. The remittance amounts can also be encrypted, and the remittance commitments can then be used in the implementation of remittance transactions. Therefore, the remittance transactions can be successfully implemented via the blockchain network, while keeping the account balance and remittance amount confidential, without affecting the blockchain nodes' verification for transaction conditions, and enabling the blockchain network to have privacy protection function.

[0069] FIG. 4 is a structure diagram of a device according to some embodiments of the specification. As shown in FIG. 4, at the level of hardware, the device comprises a processor 402, an internal bus 404, a network interface 406, an internal memory 408 and a non-volatile memory (NVM) 410. The device may further comprise other pieces of hardware. In some embodiments, the processor 402 reads corresponding computer programs from the NVM 410 to the internal memory 408 and then executes the computer programs to form an apparatus at a logical level for implementing blockchain transactions. In addition to the software implementation manner, one or more embodiments of the present specification do not exclude other implementation manners, such as a logic device or a combination of software and hardware. That is, the executive bodies of the following processing flow are not limited to logical units and may be hardware or logic devices.

[0070] Referring to FIG. 5, a block diagram of an apparatus for implementing blockchain-based transactions is provided according to some embodiments of the specification. In the software implementation manner, the apparatus for implementing blockchain-based transactions is implementable by a computing device such as remitter device and may comprise: a determination unit 501 for determining a transaction amount to be remitted from a remitter's blockchain account into a receiver's blockchain account, wherein a commitment of the remitter's balance is recorded with the remitter's blockchain

account in the blockchain, a commitment of the receiver's balance is recorded with the receiver's blockchain account in the blockchain, the commitment of the remitter's balance is calculated by using a homomorphic encryption algorithm according to a remitter's balance, and the commitment of the receiver's balance is calculated by using the homomorphic encryption algorithm according to a receiver's balance; an obtaining unit 502 for obtaining a commitment of the transaction amount which is calculated by using the homomorphic encryption algorithm according to the transaction amount; and a submission unit 503 for submitting a transaction to the blockchain, wherein the transaction comprises the information of the remitter's blockchain account, the information of the receiver's blockchain account and the commitment of the transaction amount, for the commitment of the transaction amount to be deducted from the commitment of the remitter's balance after the transaction is implemented and the commitment of the transaction amount to be added to the commitment of the receiver's balance after the transaction is implemented.

[0071] Alternatively, the commitment of the receiver's balance is calculated by using the homomorphic encryption algorithm according to the receiver's balance and a receiver random number, and the commitment of the transaction amount is calculated by using the homomorphic encryption algorithm according to the transaction amount and a transaction random number; the apparatus further comprises: a first sending unit 504 for sending the transaction random number to the receiver device via an off-chain channel for the receiver device to determine an updated receiver's balance according to an updated commitment of the receiver's balance and an updated receiver random number; wherein the updated commitment of the receiver's balance is obtained by adding the commitment of the transaction amount to the commitment of the receiver's balance, the updated receiver random number is obtained by adding the transaction random number to the receiver random number, and the updated receiver's balance is the sum of the receiver's balance and the transaction amount.

[0072] In some embodiments, the apparatus further comprises: a second sending unit 505 for sending the commitment of the transaction amount to the receiver device via an off-chain channel before submission of the transaction for the receiver device to verify association among the commitment of the transaction amount, the transaction random number and the transaction amount.

[0073] In some embodiments, the apparatus further comprises: a signature obtaining unit

506 for obtaining a receiver signature that is generated by the receiver device via a receiver private key and is related to the commitment of the transaction amount, wherein the receiver signature is generated after the associations have been verified; and a first addition unit 507 for adding the receiver signature to the transaction for the blockchain nodes in the blockchain to verify the receiver signature.

[0074] In some embodiments, the apparatus further comprises: a first generation unit 508 for generating a remitter signature related to the commitment of the transaction amount via a remitter private key; and a second addition unit 509 for adding the remitter signature to the transaction for the blockchain nodes in the blockchain to verify the remitter signature.

[0075] Alternatively, the commitment of the remitter's balance is calculated by using the homomorphic encryption algorithm according to the remitter's balance and a remitter random number, and the commitment of the transaction amount is calculated by using the homomorphic encryption algorithm according to the transaction amount and a transaction random number, wherein the transaction amount is deducted from the remitter's balance after the transaction is implemented, and the transaction random number is deducted from the remitter random number after the transaction is implemented.

[0076] In some embodiments, the apparatus further comprises: a second generation unit 510 for generating a range proof according to the remitter random number, the remitter's balance, the commitment of the remitter's balance, the transaction random number, the transaction amount and the commitment of the transaction amount; and a third addition unit 511 for adding the range proof to the transaction for the blockchain nodes in the blockchain to verify whether the transaction amount meets that: the transaction amount is not less than zero and not more than the remitter's balance.

[0077] The systems, apparatuses, modules or units illustrated in the foregoing embodiments may be implemented by computer chips or entities, or by products with certain functions. A typical device is a computer. An example of the computer may be a personal computer, a laptop computer, a cell phone, a camera phone, a smart phone, a PDA (personal digital assistant), a media player, a navigation device, an email sending and receiving device, a game console, a tablet computer, a wearable device or any combination of a few of these devices.

[0078] In a typical configuration, the computer comprises one or more processors (CPU), I/O interfaces, network interfaces and internal memories.

[0079] The internal memory may be in a form of volatile memory, random access memory (RAM) and/or non-volatile memory such as read-only memory (ROM) or flash memory (flash RAM) in the computer readable media. Internal memory is an example of computer readable media.

[0080] Computer readable media include non-volatile and volatile, movable and non-movable media, and may achieve information storage by any method or technology. Information may be computer readable instructions, data structures, program modules or other data. Examples of computer storage media include, but are not limited to, phase change random access memory (PRAM), static random access memory (SRAM), dynamic random access memory (DRAM) and other types of random access memory (RAM), read only memory (ROM), electrically erasable programmable read only memory (EEPROM), flash memory or other memory technologies, compact disc–read only memory (CD-ROM), digital versatile disc (DVD) or other optical memory, cassette type magnetic tape, magnetic disk memory, quantum memory, graphene-based storage media, or other magnetic storage devices or any other non-transfer media, which may be used to store information that is accessible to computation devices. According to the specification, computer readable media do not include transitory media, such as modulated data signals and carriers.

[0081] Terms “include,” “contain” or any other variants of these terms are intended to cover non-exclusive inclusion so that a process, method, commodity or device including a series of elements not only includes these elements but also includes other elements not clearly set out, or also include the elements inherent to such process, method, commodity or device. Unless otherwise with more limitations, the elements defined by “include one.....” do not exclude that the process, method, commodity or device including the elements also have other same elements.

[0082] Embodiments of the present specification are described above. Other embodiments are in the scope of the attached claims. In some embodiments, the actions or steps recorded in the claims may be executed in a sequence different from that given in the embodiments and can still achieve the expected results. Further, it is not necessary for the process described in the accompanying drawings to require the given specific sequence or a continuous sequence to achieve the expected results. In some embodiments, multitasking processing and parallel processing are also acceptable or may be favorable.

[0083] The terms used in one or more embodiments of the present specification are only for

the purpose of describing embodiments and not intended to limit one or more embodiments of the present specification. The singular forms “one,” “the” and “this” used in one or more embodiments of the present specification and in the attached claims also are intended to cover plural forms unless other meanings are clearly indicated in the context. The term “and/or” used in the text refers to any or all possible combinations containing one or more the associated listed items.

[0084] Although one or more embodiments of the present specification may use terms such as first, second and third to describe various kinds of information, the information should not be limited to these terms. These terms are only intended to differentiate information of the same type. For example, without departing from the scope of one or more embodiments of the present specification, first information may also be referred to as second information, and similarly, second information may also be referred to as first information. Subject to the context, the term “if” used here may be interpreted as “at the time of ...,” “when ...,” or “in response to determination.”

[0085] The foregoing description is not intended to limit one or more embodiments of the present specification. Any modifications, equivalent replacements and improvements made without departing from the spirit and principle of one or more embodiments of the present specification shall fall within the scope of one or more embodiments of the present specification.

What is claimed is:

1. A method for implementing blockchain-based transactions, implementable by a computing device associated with a remitter, the method comprising:

determining a transaction amount to be remitted from the remitter's blockchain account into a receiver's blockchain account, wherein a commitment of the remitter's balance is recorded with the remitter's blockchain account in a blockchain, a commitment of the receiver's balance is recorded with the receiver's blockchain account in the blockchain, the commitment of the remitter's balance is calculated by using a homomorphic encryption algorithm according to the remitter's balance, and the commitment of the receiver's balance is calculated by using the homomorphic encryption algorithm according to the receiver's balance;

obtaining a commitment of the transaction amount by using the homomorphic encryption algorithm according to the transaction amount; and

submitting to the blockchain a transaction comprising information of the remitter's blockchain account, information of the receiver's blockchain account, and the commitment of the transaction amount, for the commitment of the transaction amount to be deducted from the commitment of the remitter's balance and the commitment of the transaction amount to be added to the commitment of the receiver's balance after the transaction is implemented by the blockchain,

wherein:

the commitment of the receiver's balance is calculated by using the homomorphic encryption algorithm according to the receiver's balance and a first random number; and

the commitment of the transaction amount is calculated by using the homomorphic encryption algorithm according to the transaction amount and a transaction random number, and

before submitting the transaction, the method further comprises sending the transaction random number to another computing device associated with the receiver via an off-chain channel, to cause the computing device associated with the receiver to determine an updated receiver's balance according to an updated commitment of the receiver's balance and an updated first random number.

2. The method as described in claim 1, wherein:

the updated commitment of the receiver's balance is a sum of the commitment of the transaction amount and the commitment of the receiver's balance.

3. The method as described in any of the claims 1-2, wherein:

the updated first random number is a sum of the transaction random number and the first random number.

4. The method as described in any of the preceding claims, wherein:

the updated receiver's balance is a sum of the receiver's balance and the transaction amount.

5. The method as described in any of the preceding claims, before submitting the transaction, further comprising:

sending the commitment of the transaction amount to the computing device associated with the receiver via the off-chain channel for the computing device associated with the receiver to verify an association among the commitment of the transaction amount, the transaction random number, and the transaction amount.

6. The method as described in claim 5, before submitting the transaction, further comprising:

obtaining a receiver signature generated by the computing device associated with the receiver based on a receiver private key and related to the commitment of the transaction amount, wherein the receiver signature is generated after the association has been verified; and

adding the receiver signature to the transaction for the blockchain nodes in the blockchain to verify the receiver signature.

7. The method as described in any preceding claim, before submitting the transaction, further comprising:

generating a remitter signature related to the commitment of the transaction amount based on a remitter private key; and

adding the remitter signature to the transaction for the blockchain nodes in the blockchain to verify the remitter signature.

8. The method as described in any preceding claim, wherein:

the commitment of the remitter's balance is calculated by using the homomorphic encryption algorithm according to the remitter's balance and a second random number.

9. The method as described in claim 8, wherein for the blockchain to implement the transaction, the transaction amount is deducted from the remitter's balance; and the transaction random number is deducted from the second random number after the transaction is implemented.

10. The method as described in any of the claims 8-9, before submitting the transaction, further comprising:

generating a range proof according to the second random number, the remitter's balance, the commitment of the remitter's balance, the transaction random number, the transaction amount, and the commitment of the transaction amount; and

adding the range proof to the transaction for the blockchain nodes in the blockchain to verify whether the transaction amount is not less than zero and not more than the remitter's balance.

11. A system for implementing blockchain-based transactions, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 10.

12. An apparatus for implementing blockchain-based transactions, comprising a plurality of modules for performing the method of any claims 1 to 10.

13. A non-transitory computer-readable storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform the method of any of claims 1 to 10.