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. 201810887463.2, 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 blockchains, particularly to a method, apparatus, and electronic device for implementing blockchain-based transactions.

BACKGROUND ART

[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 is provided for implementing blockchain-based transactions. The method may comprise: selecting one or more blockchain assets from a remitter's blockchain account according to a transaction amount of a transaction to be remitted from the remitter's blockchain account into a receiver's blockchain account, wherein a total asset amount represented by the selected one or more blockchain assets is not less than the transaction amount, and a commitment of an individual asset amount represented by each of the selected one or more blockchain assets is recorded in a blockchain; generating a commitment of the transaction amount; and submitting to the blockchain the transaction comprising information of the selected one or more blockchain assets and the commitment of the transaction amount, for the selected one or more blockchain assets to be removed from the remitter's blockchain account and one or more blockchain assets corresponding to the commitment of the

transaction amount to be added to the receiver's blockchain account.

[0006] In some embodiments, the commitment of the transaction amount is obtained by applying an encryption algorithm to the transaction amount and a transaction random number, and wherein the computing device is associated with the remitter, and the method may further comprise: before submitting the transaction to the blockchain, 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, according to the encryption algorithm and the transaction random number, a transaction asset amount represented by the one or more blockchain assets to be added to the receiver's blockchain account. In some embodiments, the encryption algorithm may be Pedersen Commitment.

[0007] In some embodiments, before submitting the transaction to the blockchain, the method may further comprise: sending the commitment of the transaction amount to the computing device associated with the receiver via an 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 to the blockchain, the method may further comprise: obtaining a receiver signature generated by the computing device associated with the receiver based on a receiver private key after successfully verifying the association, wherein the receiver signature represents the receiver's endorsement for the commitment of the transaction amount; and adding the receiver signature to the transaction for blockchain nodes in the blockchain to verify the receiver signature.

[0009] In some embodiments, the method may further comprise: generating a remitter signature related to the commitment of the transaction amount via a remitter private key; and adding the remitter signature to the transaction for blockchain nodes in the blockchain to verify the remitter signature.

[0010] In some embodiments, the method may further comprise: generating a range proof, wherein the range proof is related to the transaction amount; and adding the range proof to the transaction.

[0011] In some embodiments, before submitting the transaction to the blockchain, the method may further comprise: generating a commitment of a change amount in response to

the total asset amount represented by the selected one or more blockchain assets being more than the transaction amount, wherein the change amount is a difference between the total asset amount of the selected one or more blockchain assets and the transaction amount; and adding the commitment of the change amount to the transaction, for one or more blockchain assets corresponding to the commitment of the change amount to be credited back to the remitter's blockchain account.

[0012] In some embodiments, the commitment of the individual asset amount (Mi) is obtained by applying a homomorphic encryption algorithm to the individual asset amount (pi) and an asset random number (ri), wherein $0<i\leqslant k$ and k is the number of the selected one or more blockchain assets; the commitment of the transaction amount (T) is obtained by applying the homomorphic encryption algorithm to the transaction amount (t) and a transaction random number (r); the commitment of the change amount (T0) is obtained by applying the homomorphic encryption algorithm to the change amount (t0) and a change random number (r0); and before submitting the transaction to the blockchain, the method may further comprise: generating a verification random number (r'), wherein r'=r1+……+rk-r-r0; and adding the verification random number (r') to the transaction for blockchain nodes in the blockchain to verify whether an input of the transaction is equal to an output of the transaction.

[0013] In some embodiments, the input of the transaction is verified to be equal to the output of the transaction in response to a verification commitment (R') corresponding to the verification random number r' is equal to M1+……+Mk-T-T0.

[0014] In some embodiments, the commitment of the change amount is obtained by applying the homomorphic encryption algorithm to the change amount and a change random number.

[0015] In some embodiments, before submitting the transaction to the blockchain, the method may further comprise: generating a range proof, wherein the range proof is related to the change amount; and adding the range proof to the transaction.

[0016] According to a second aspect of one or more embodiments of the present specification, an apparatus is provided for implementing blockchain-based transactions. 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 apparatus to perform operations

comprising: selecting one or more blockchain assets from a remitter's blockchain account according to a transaction amount of a transaction to be remitted from the remitter's blockchain account into a receiver's blockchain account, wherein a total asset amount represented by the selected one or more blockchain assets is not less than the transaction amount, and a commitment of an individual asset amount represented by each of the selected one or more blockchain assets is recorded in a blockchain; generating a commitment of the transaction amount; and submitting to the blockchain the transaction comprising information of the selected one or more blockchain assets and the commitment of the transaction amount, for the selected one or more blockchain assets to be removed from the remitter's blockchain account and one or more blockchain assets corresponding to the commitment of the transaction amount to be added to the receiver's blockchain account.

[0017] 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 configured with instructions executable by one or more processors to cause the one or more processors to perform operations comprising: selecting one or more blockchain assets from a remitter's blockchain account according to a transaction amount of a transaction to be remitted from the remitter's blockchain account into a receiver's blockchain account, wherein a total asset amount represented by the selected one or more blockchain assets is not less than the transaction amount, and a commitment of an individual asset amount represented by each of the selected one or more blockchain assets is recorded in a blockchain; generating a commitment of the transaction amount; and submitting to the blockchain the transaction comprising information of the selected one or more blockchain assets and the commitment of the transaction amount, for the selected one or more blockchain assets to be removed from the remitter's blockchain account and one or more blockchain assets corresponding to the commitment of the transaction amount to be added to the receiver's blockchain account.

BRIEF DESCRIPTION OF THE DRAWING

[0018] FIG. 1 is a flow chart of a method for implementing blockchain-based transactions according to some embodiments of the specification.

[0019] FIG. 2 is a schematic diagram of an implementation of a remittance transaction in a blockchain network according to some embodiments of the specification.

[0020] FIG. 3 is a flow chart of an implementation of a remittance transaction in a

blockchain network according to some embodiments of the specification.

[0021] FIG. 4 is a schematic structural diagram of a device for implementing blockchain-based transactions according to some embodiments of the specification.

[0022] FIG. 5 is a block diagram of an apparatus for implementing blockchain-based transactions according to some embodiments of the specification.

DETAILED DESCRIPTION

[0023] 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.

[0024] 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.

[0025] 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.

[0026] A remitter device refers to a computing device associated with a remitter who remits money to a receiver through one or more transactions. A receiver device refers to a computing device associated with a receiver who receives money from a remitter through one or more transactions. 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.

[0027] Step 102, selecting one or more blockchain assets from a remitter's blockchain account according to a transaction amount of a transaction to be remitted from the remitter's blockchain account into a receiver's blockchain account, where a total asset amount represented by the selected one or more blockchain assets is not less than the transaction amount, and a commitment of an individual asset amount represented by each of the selected one or more blockchain assets is recorded in the blockchain.

[0028] In some embodiments, an "account balance" in a blockchain account may include one or more types of blockchain assets that may be applied respectively in different transactions. In one embodiment, the blockchain account may participate in multiple transactions in parallel, which significantly improves the transaction efficiency for blockchain-based transactions. For example, assuming that a remitter's blockchain account simultaneously contains blockchain assets 1-5, blockchain assets 1-3 may be tapped in transaction 1, while blockchain assets 4-5 may be tapped in transaction 2. Transactions 1 and 2 may be executed at the same time, instead of in sequence.

[0029] In some embodiments, a blockchain account contains multiple blockchain assets which are added respectively to the blockchain account via transactions, and the transactions may be executed by the owner of the blockchain account or any other user.

[0030] In some embodiments, a blockchain account may not actively combine blockchain assets or split a blockchain asset, while the owner may actively combine blockchain assets or split a blockchain asset in the blockchain account.

[0031] In some embodiments, the blockchain nodes in a blockchain may respectively maintain unified blockchain ledgers based on a consensus. Information of the blockchain assets contained in the blockchain accounts (for example, the foregoing remitter's blockchain accounts and the receiver's blockchain accounts) is recorded in the blockchain ledgers. In some embodiments, the blockchain ledgers record a commitment of an individual asset amount corresponding to each of the blockchain assets, and may not record the individual asset amount in order to keep the balances of the corresponding blockchain accounts confidential.

[0032] In some embodiments, each blockchain asset may comprise an asset certificate. The asset certificate may correspond to a token, a digital asset, or any other intelligent asset in a

blockchain. Alternatively, the asset certificate may correspond to cash, security, a discount coupon, a real estate, and any other asset not in the blockchain.

[0033] Step 104, generating a commitment of the transaction amount.

[0034] In some embodiments, generating a commitment of the transaction amount allows the blockchain ledgers to record the commitment of the transaction amount but not to record the transaction amount, so that the transaction amount is kept confidential in the course of transaction.

[0035] Step 106, submitting a transaction to the blockchain, where the transaction may contain the information of the selected blockchain assets and the commitment of the transaction amount, so that the selected blockchain assets are removed from the remitter's blockchain account after the transaction is implemented and blockchain assets corresponding to the commitment of the transaction amount are added to the receiver's blockchain account after the transaction is implemented.

[0036] In some embodiments, the commitment of the transaction amount may be calculated by a predetermined encryption algorithm according to the transaction amount and a transaction random number. A transaction random number may refer to a random number used to generate a commitment of the transaction amount based on an encryption algorithm, such as a homomorphic encryption algorithm. Correspondingly, a remitter device may send the transaction random number to a receiver device via an off-chain channel so that the receiver device can determine a transaction asset amount represented by the one or more blockchain assets to add to the receiver's blockchain account according to the predetermined encryption algorithm and the transaction random number. Transmitting the transaction random number via an off-chain channel may avoid the transaction random number being recorded in the blockchain ledgers, ensuring that the transaction amount is kept confidential. After the blockchain executes the transaction, the receiver device may decrypt the encrypted transaction asset amount (e.g., the commitment of the transaction amount) based on the transaction random number to obtain the transaction asset amount of the blockchain assets added to the receiver's blockchain account and optionally apply the blockchain assets added to the receiver's blockchain account in a subsequent transaction process.

[0037] 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 to the blockchain so that the receiver device verifies an association among the commitment of the

transaction amount, the transaction random number, and the transaction amount. A receiver device may allow 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; otherwise may not provide this receiver signature.

[0038] In some embodiments, a remitter device may obtain a receiver signature. The receiver signature is generated by a receiver device based on a receiver private key and is related to the commitment of the transaction amount. The receiver signature may represent receiver device's endorsement for the commitment of the transaction amount. In some embodiments, the receiver signature is generated by the receiver device after the above-described association has been verified; the receiver signature is then added to the transaction so that the blockchain nodes in the blockchain can 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.

[0039] In some embodiments, a remitter device may generate a remitter signature related to the commitment of the transaction amount via a remitter private key, and add the remitter signature to the transaction so that the blockchain nodes in the blockchain can verify the remitter signature. For example, when a transaction does not contain the remitter signature, the blockchain nodes may determine that consensus fails, thereby refusing to proceed with the transaction.

[0040] In some embodiments, a remitter device may generate a range proof, wherein the range proof is related to 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. A range proof is a form of commitment validation that enables verifying that a commitment represents an amount within a specified range, without revealing the amount. For example, the range proof related to the transaction random number, the transaction amount, and the commitment of the transaction amount may enable verifying that the commitment represents the transaction amount which is not less than zero. For instance, range proof technologies such as a Bulletproofs solution or a Borromean ring signature solution may be used. Those of ordinary skill in the art should also appreciate that other example of range proof technologies may be applied.

[0041] In some embodiments, the asset amount represented by the selected blockchain assets may be equal to or greater than the transaction amount. When the asset amount is equal to the transaction amount, the selected blockchain assets may be removed from the remitter's blockchain account after the transaction is implemented, and the blockchain assets corresponding to the commitment of the transaction amount may be added to the receiver's blockchain account after the transaction is implemented.

[0042] In some embodiments, when the asset amount is more than the transaction amount, the selected blockchain assets may similarly be removed from the remitter's blockchain account after the transaction is implemented. In some embodiments, a change amount (e.g., a difference between the asset amount and the transaction amount) may be credited back to the remitter's blockchain account. The blockchain assets corresponding to the commitment of the transaction amount may be added to the receiver's blockchain account after the transaction is implemented.

[0043] In some embodiments, a remitter device may generate a commitment of a change amount when the asset amount represented by the selected blockchain assets is more than the transaction amount. The change amount is the difference between the asset amount represented by the selected blockchain assets and the transaction amount. In addition, the remitter device may add the commitment of the change amount to the transaction so that the blockchain assets corresponding to the commitment of the change amount are added to the remitter's blockchain account after the transaction is implemented, thereby ensuring that the remitted amount of the blockchain assets is equal to the received amount.

[0044] In some embodiments, a commitment of an individual asset amount Mi is obtained by applying a homomorphic encryption algorithm to the asset amount pi represented by a selected blockchain asset Pi and an asset random number ri, where $0<i\leq k$ and k is the number of the selected blockchain assets. The commitment of the transaction amount T is obtained by applying the homomorphic encryption algorithm to the transaction amount t and the transaction random number r, and the commitment of the change amount T0 is obtained by applying the homomorphic encryption algorithm to the change amount t0 and the change random number r0. A remitter device may generate a verification random number r', where r'=r1+……+rk-r-r0; and add the verification random number r' in the transaction so that the blockchain nodes in the blockchain can verify whether the input of the transaction is equal to the output of the transaction. In some embodiments, the input of the transaction is verified to

be equal to the output of the transaction when the verification commitment R', to which the verification random number r' corresponds, satisfies the equation: R'=M1+……+Mk-T-T0.

[0045] In some embodiments, any type of homomorphic encryption algorithm may be used to obtain the above-described commitments. For example, any homomorphic encryption algorithm satisfying additive homomorphism and supporting a proof that a piece of plaintext data belongs to a range may be used. Therefore, the blockchain nodes can conduct subtraction and addition to the ciphertext encrypted by homomorphic encryption, determine R'=M1+……+Mk-T-T0 according to r'=r1+……+rk-r-r0, and also provide a proof regarding the ciphertext to prove that the transaction amount is not less than zero and not more than the total amount of the assets in the transaction. In some examples, the homomorphic encryption algorithm may be an additively homomorphic encryption algorithm or a fully homomorphic encryption algorithm. For example, the homomorphic encryption algorithm may be a Pedersen commitment mechanism. The present specification has no limitation to this.

[0046] In some embodiments, the commitment of the change amount is calculated by a homomorphic encryption algorithm according to the change amount and a change random number. A remitter device may generate a range proof related to the change random number, the change amount, and the commitment of the change amount. For example, the range proof may enable proving that the commitment represents the change amount which is not less than zero. The remitter device may add the range proof to the transaction, so that the blockchain nodes in the blockchain can verify whether the change amount is not less than zero. For instance, range proof technologies such as a Bulletproofs solution or a Borromean ring signature solution may be used. Those of ordinary skill in the art should also appreciate that other example of range proof technologies may be applied.

[0047] In some embodiments, another range proof may be related to all of the transaction random number, the transaction amount, the commitment of the transaction amount, the change random number, the change amount, and the commitment of the change amount. The range proof may enable verifying that the commitment of the transaction amount represents the transaction amount which is not less than zero, and that the commitment of the change amount represents the change amount which is not less than zero. A remitter device may add the range proof to the transaction, so that the blockchain nodes can verify based on the range proof whether both the transaction amount and the change amount are not less than zero.

[0048] 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.

[0049] 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 login user account, while this user account may belong to an individual or an organization.

[0050] 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.

[0051] A client program of blockchain may be executed on the user device 1 so that the user device 1 corresponds to 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 corresponds to 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 k 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.

[0052] 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.

[0053] Step 301, the remitter drafts a remittance transaction.

[0054] In some embodiments, a remitter may refer to an individual or entity that remits a fund and other resources in a remittance transaction; correspondingly, a receiver may refer to an individual or entity that receives a fund and/or other resources in a 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.

[0055] In some embodiments, when drafting a remittance transaction, the remitter may negotiate a to-be-remitted amount t with the receiver. The remitter may select k notes P1~pk from the blockchain account 1 corresponding to a user A. A "note" refers to a blockchain asset of certain an asset amount. Each blockchain account in the present specification may contain multiple notes. Note information of each note in the blockchain account may include a NoteType field, a NoteID field, and a field of a commitment of an asset amount. The NoteType field stands for an asset type of the corresponding note, the NoteID field stands for an unique identification of the corresponding note, and the field of the commitment of the asset amount stands for the commitment of the asset amount generated based on the asset amount of the note via a Pedersen commitment mechanism, etc.

[0056] In some embodiments, the transaction model used in the present specification may include a transaction address TxID field, a signature field, an input field, and an output field. For example, the TxID field is a hash value of transaction content, the signature field includes a remitter's signature and a receiver's signature, the input field includes an account address of the remitter's blockchain account corresponding to the remitter and a list of selected notes in the remitter's blockchain account, and the output field includes an output information list. For example, the list contains multiple items arranged in sequence, where each item has a corresponding serial number Index, and each item includes: an account address of the receiver's blockchain account, a type of an asset to be received and a commitment of an asset amount to be received; the "receiver" may be the party in the remittance operation for receiving the blockchain asset corresponding to a to-be-remitted amount or a change that is associated with the to-be-remitted amount. For example, the remitter may also simultaneously be "receiver" for receiving the blockchain asset corresponding to a change amount. In the NoteID field corresponding to the foregoing note, the value of NoteID may be calculated by adding the address TxID of the transaction generating the note and a corresponding serial number Index of the note in the output information list of the transaction.

[0057] In some embodiments, according to the asset type of the to-be-remitted amount t, the remitter may select a number of notes of the same asset type from the remitter's blockchain account and ensure that the sum of the asset amounts represented by the selected notes is not less than the to-be-remitted amount t. If the notes of the same asset type are not sufficient to complete the remittance, the remitter may abandon the remittance, or may use the notes of other asset types for the remittance according to an exchange rate. For easier understanding, the terms involving the amount of assets, such as asset amount, refer to the value after conversion according to a corresponding exchange rate hereinafter.

[0058] In some embodiments, it is assumed that the asset amounts corresponding to notes P1~pk are p1~pk, and notes P1~pk correspond to asset random numbers r1~rk respectively. The asset amounts p1~pk and the asset random numbers r1~rk may be used to generate corresponding commitments of the asset amounts M1~mk respectively according to homomorphic encryption based on a Pedersen commitment mechanism, etc., where Mi=Comm(ri, pi)=ri×G+pi×H, and G and H are known functions (such as a generator for randomly generating elliptic curves).

[0059] In some embodiments, a user device 1 may read the commitments of the asset amounts M1~mk corresponding to the notes P1~pk respectively from the blockchain ledger maintained by a node 1, and decrypt the commitments of the asset amounts M1~mk to obtain corresponding asset amounts p1~pk, based on the asset random numbers r1~rk corresponding to the notes P1~pk, respectively, which are known to the user device 1, so as to ensure p1+p2+……+pk ≥ to-be-remitted amount t. In addition, the user device 1 may also calculate the change amount t0=p1+p2+……+pk-t.

[0060] In some embodiments, the user device 1 may generate a transaction random number r for the to-be-remitted amount t, and a change random number r0 for the change amount t0, and conduct homomorphic encryption to the to-be-remitted amount t and the transaction random number r based on a Pedersen commitment mechanism, etc., to obtain a commitment of the to-be-remitted amount T=Comm(r, t), and conduct homomorphic encryption to the change amount t0 and the change random number r0 to obtain a commitment of the change amount T0=Comm(r0, t0).

[0061] Step 302, the remitter sends (r, t, T) to a receiver via an off-chain channel.

[0062] In some embodiments, sending (r, t, T) via an off-chain channel rather than a blockchain network may avoid recording the transaction random number r and the to-be-

remitted amount t in a blockchain ledger, and ensure that the to-be-remitted amount t is unknown except to the remitter and the receiver.

[0063] Step 303, the receiver verifies the received (r, t, T).

[0064] In some embodiments, the receiver may verify the to-be-remitted amount t to determine that it is the negotiated to-be-remitted amount. In some embodiments, when the to-be-remitted amount t is correct, the receiver may verify the commitment of the to-be-remitted amount T; in other words, the receiver may calculate the transaction random number r and the to-be-remitted amount t via the encryption algorithm based on a Pedersen commitment mechanism to verify if the commitment of the to-be-remitted amount T=Comm(r, t) is correct. If yes, the verification is passed. If not, the verification is not passed.

[0065] Step 304, after the verification is passed, a signature SIGB is generated and returned to the remitter.

[0066] 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 to the remittance transaction with a commitment T implemented from the blockchain account 1 of the user A to the blockchain account 2 of user B.

[0067] Step 305, after receiving the signature SIGB, the remitter generates a range proof PR.

[0068] In some embodiments, in order to ensure that a remittance transaction is completed smoothly, blockchain nodes may determine that the remittance transaction meets the following conditions: $t \geq 0$ and $t0 \geq 0$. In some embodiments, range proof technologies enable the blockchain nodes to verify the range proof PR in a ciphertext state to determine whether the remittance transaction meets the foregoing conditions. For example, range proof technologies such as a Bulletproofs solution or a Borromean ring signature solution may be used. Those of ordinary skill in the art should also appreciate that other example of range proof technologies may be applied.

[0069] In some embodiments, the remitter may use a range proof technology to generate a range proof PR related to (r0, t0, T0, r, t, T) to enable the blockchain nodes to verify whether $t \geq 0$ and $t0 \geq 0$ in the subsequent process.

[0070] Step 306, the remitter generates a signature SIGA.

[0071] In some embodiments, the remitter may use a remitter private key to sign (A:P1,P2……,Pk;A:T0;B:T;PR,r') and generate a signature SIGA, where r'=r1+……+rk-r-r0.

[0072] Step 307, the remitter submits the transaction to the blockchain.

[0073] In some embodiments, the remitter submits a corresponding remittance transaction (A:P1,P2……,Pk;A:T0;B:T;PR,r';SIGA,SIGB) to the blockchain via a node 1 to execute this remittance transaction. The remittance transaction (A:P1,P2……,Pk;A:T0;B:T;PR,r';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:P1,P2……,Pk;A:T0;B:T;PR,r';SIGA,SIGB) respectively to execute the remittance operation when the verification is passed, or to refuse the remittance when the verification is not passed.

[0074] Step 308, the blockchain nodes check if the transaction has been executed.

[0075] In some embodiments, the blockchain nodes may be any blockchain nodes in a blockchain network. In other words, every blockchain node in the blockchain network may receive the remittance transaction (A:P1,P2……,Pk;A:T0;B:T;PR,r';SIGA,SIGB), and perform verification and other operations through Steps 308-313.

[0076] In some embodiments, after the blockchain nodes receive the remittance transaction (A:P1,P2……,Pk;A:T0;B:T;PR,r';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 the remittance transaction (A,B,T;SIGA,SIGB;PR) may be rejected, otherwise the process proceeds to Step 309.

[0077] Step 309, the blockchain nodes check signatures.

[0078] In some embodiments, the blockchain nodes may check if signatures SIGA and SIGB contained in the remittance transaction (A:P1,P2……,Pk;A:T0;B:T;PR,r';SIGA,SIGB) are correct. If the signatures are not correct, the execution of this remittance transaction (A:P1,P2……,Pk;A:T0;B:T;PR,r';SIGA,SIGB) may be rejected, otherwise the process proceeds to Step 310.

[0079] Step 310, the blockchain nodes check if the asset types are consistent.

[0080] In some embodiments, the blockchain nodes check the NoteType fields of the notes

P1~pk to determine the asset types of the blockchain assets represented by the notes P1~pk; when the asset types corresponding to P1~pk are inconsistent with the designated remittance types (the asset types used by the to-be-remitted amounts), the execution of this remittance transaction (A:P1,P2……,Pk;A:T0;B:T;PR,r';SIGA,SIGB) may be rejected, otherwise the process proceeds to Step 311.

[0081] In other embodiments, even if the asset types are inconsistent, as long as the remitter has converted the asset amounts represented by the notes according to the relevant exchange rate when calculating T0, PR, r', and other parameters, then Step 310 may be skipped.

[0082] Step 311, the blockchain nodes the check range proof PR.

[0083] In some embodiments, the blockchain nodes may, based on a range proof technology, check the range proof PR contained in the remittance transaction (A:P1,P2……,Pk;A:T0;B:T;PR,r';SIGA,SIGB) to determine whether the conditions of $t \geq 0$ and $t0 \geq 0$ are met. If the conditions are not met, the execution of this remittance transaction (A:P1,P2……,Pk;A:T0;B:T;PR,r';SIGA,SIGB) may be rejected; otherwise the process proceeds to Step 312.

[0084] Step 312, the blockchain nodes check if the input and the output are equal.

[0085] In some embodiments, because r'=r1+……+rk-r-r0, then according to the characteristics of the homomorphic encryption mechanism, the asset amount corresponding to r' is t'= p1+……+pk-t-t0; since the input of the remittance transaction is the sum of the asset amounts p1~pk corresponding to the selected notes P1~Pk, namely p1+……+pk, and the output is the sum of the to-be-remitted amount and the change amount, namely t+t0, then the condition of p1+……+pk=t+t0 is met when the input is equal to the output, enabling t'= p1+……+pk-t-t0=0. Therefore, the commitment corresponding to r' is Comm(r', t')=r'×G+t'×H= r'G. According to r'=r1+……+rk-r-r0, the blockchain nodes may verify whether r'G is equal to M1+……+Mk-T-T0 corresponding to r1+……+rk-r-r0 to determine whether the input is equal to the output; it is determined that the input is equal to the output when r'G= M1+……+Mk-T-T0; otherwise the input and output are not equal.

[0086] Step 313, the blockchain nodes check if the remitter holds related notes.

[0087] In some embodiments, the blockchain nodes may determine whether the notes selected and designated in the transaction are included in the remitter's blockchain account according to the information related to the remitter's blockchain account (for example, the

blockchain account corresponding to the user A) recorded in the maintained blockchain ledgers. If the notes are included, it is determined that the remitter holds the related notes; otherwise the remitter does not hold the notes.

[0088] Step 314, in the maintained blockchain ledgers, the blockchain nodes update the balances in the blockchain accounts to which the user A and the user B correspond respectively.

[0089] In some embodiments, it is assumed that the user A corresponds to the blockchain account 1 and the user B corresponds to the blockchain account 2; after the verification in Steps 308-313 is passed, the blockchain nodes may update the notes held by the blockchain account 1 and the blockchain account 2 in the maintained blockchain ledgers respectively: deleting notes P1~pk input in the transaction from and crediting back a note corresponding to the commitment of the change amount T0 to the blockchain account 1, and adding a note corresponding to the commitment of the to-be-remitted amount T to the blockchain account 2.

[0090] Based on the properties of homomorphic encryption algorithms, due to the commitment of the change amount T0=Comm(r0,t0) and because the user device 1 knows r0 and can learn that the commitment of a new note from the blockchain ledger maintained by the node 1 is T0, the asset amount represented by the note can be decrypted to obtain t0. Similarly, because the commitment of the to-be-remitted amount T=Comm(r, t) and the user device 2 obtains the transaction random number r notified by the remitter in Step 302 and can learn that the commitment of a new note from the blockchain ledger maintained by the node 2 is T, therefore the asset amount represented by the note may be decrypted to obtain t.

[0091] To sum up, the adoption of the account model based on a note mechanism allows the same blockchain account to contain multiple notes that can be used in multiple parallel remittance transactions respectively, thereby significantly improving transaction efficiency. At the same time, the use of the homomorphic encryption mechanism allows the encryption of the asset amount represented by the notes contained in the blockchain accounts. After encryption of the asset amount, the commitment of the asset amount may be recorded in blockchain ledgers. The to-be-remitted amount, the change amount, etc., can also be encrypted in remittance transactions, and the commitment of the to-be-remitted amount and commitment of the change amount 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, the remitted balance and the change amount confidential, without affecting the blockchain nodes' verification of transaction conditions, and enabling the blockchain network to have a privacy protection function.

[0092] FIG. 4 is a schematic structural diagram of a device according to some embodiments of the specification. As shown in FIG. 4, at the hardware level, the device comprises a processor 402, an internal bus 404, a network interface 406, an internal memory 408 and a nonvolatile memory (NVM) 410. In some embodiments, the device may further comprise other pieces of hardware for transactions. In some embodiments, the processor 402 reads a corresponding computer program from the NVM 410 to the internal memory 408 and then executes the computer program to form a terminal interaction apparatus at a logical level. 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.

[0093] Referring to FIG. 5, a block diagram of an apparatus for implementing blockchain-based transactions is provided according to some embodiments of the specification. As shown in FIG. 5, in the software implementation manner, the terminal interaction apparatus is implementable by computing devices as remitter devices and may comprise: a selection unit 501 for selecting one or more blockchain assets from a remitter's blockchain account according to a transaction amount of a transaction to be remitted from the remitter's blockchain account into the receiver's blockchain account; wherein a total asset amount represented by the selected one or more blockchain assets is not less than the transaction amount, and a commitment of an individual asset amount represented by each of the selected one or more blockchain assets is recorded in the blockchain; a first generation unit 502 for generating a commitment of the transaction amount; and a submission unit 503 for submitting a transaction to the blockchain, wherein the transaction contains the information of the selected one or more blockchain assets and the commitment of the transaction amount, for the selected one or more blockchain assets to be removed from the remitter's blockchain account after the transaction is implemented and one or more blockchain assets corresponding to the commitment of the transaction amount to be added to the receiver's blockchain account after the transaction is implemented.

[0094] In some embodiments, the commitment of the transaction amount is obtained by

applying a predetermined encryption algorithm to the transaction amount and a transaction random number, and the apparatus further comprises: a first sending unit 504 for sending the transaction random number to a receiver device via an off-chain channel so that the receiver device determines a transaction asset amount represented by the blockchain assets to be added into the receiver's blockchain account according to the predetermined encryption algorithm and the transaction random number.

[0095] 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 so that the receiver device verifies an association among the commitment of the transaction amount, the transaction random number and the transaction amount.

[0096] In some embodiments, the apparatus further comprises: an 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 by the receiver device after the association has been verified; and a first addition unit 507 for adding the receiver signature to the transaction so that the blockchain nodes in the blockchain conduct signature verification to verify the receiver signature.

[0097] In some embodiments, the apparatus further comprises: a second 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 so that the blockchain nodes in the blockchain conduct signature verification to verify the remitter signature.

[0098] In some embodiments, the apparatus further comprises: a third generation unit 510 for generating a range proof, wherein the range proof is related to 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 so that the blockchain nodes in the blockchain verify whether the transaction amount is not less than zero.

[0099] In some embodiments, the apparatus further comprises: a fourth generation unit 512 for generating a commitment of a change amount when the asset amount represented by the selected blockchain assets is more than the transaction amount, wherein the change amount is the difference between the asset amount represented by the selected blockchain assets and the

transaction amount; and a fourth addition unit 513 for adding the commitment of the change amount to the transaction, for the blockchain assets corresponding to the commitment of the change amount to be added to the remitter's blockchain account after the transaction is implemented.

[00100] In some embodiments, a commitment of an individual asset amount Mi is obtained by applying a homomorphic encryption algorithm to the individual asset amount pi represented by a selected blockchain asset Pi and an asset random number ri, where $0<i\leq k$ and k is the number of the selected blockchain assets, the commitment of the transaction amount T is calculated by using the homomorphic encryption algorithm according to the transaction amount t and the transaction random number r, and the commitment of the change amount T0 is calculated by using the homomorphic encryption algorithm according to the change amount t0 and a change random number r0; and the apparatus further comprises: a fifth generation unit 514 for generating a verification random number r', wherein r'=r1+……+rk-r-r0; and a fifth addition unit 515 for adding the verification random number r' into the transaction so that the blockchain nodes in the blockchain verify whether the input of the transaction is equal to the output of the transaction, wherein the input of the transaction is verified to be equal to the output of the transaction when the verification commitment R', to which the verification random number r' corresponds, satisfies the equation: R'=M1+……+Mk-T-T0.

[00101] In some embodiments, the commitment of the change amount is obtained by applying a homomorphic encryption algorithm to the change amount and a change random number, and the apparatus further comprises: a sixth generation unit 516 for generating a range proof, wherein the range proof is related to the change random number, the change amount and the commitment of the change amount; and a sixth addition unit 517 for adding the range proof to the transaction so that the blockchain nodes in the blockchain verify whether the change amount is not less than zero.

[00102] The systems, apparatuses, modules or units illustrated in the foregoing embodiments may be achieved 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.

[00103] In a typical configuration, the computer comprises one or more processors (CPU), I/O interfaces, network interfaces and internal memories.

[00104] 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.

[00105] 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), 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 computing devices. According to the specification, computer readable media do not include transitory media, such as modulated data signals and carriers.

[00106] It should be further noted that 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. In the absence of more limitations, the elements defined by a sentence "include one……" do not exclude that the process, method, commodity or device including the elements also have other identical elements.

[00107] 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 in order to achieve the expected results. In some embodiments, multitasking processing and

parallel processing are also acceptable or may be favorable.

[00108] 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. It should also be understood that the term “and/or” used in the text refers to any or all possible combinations containing one or more the associated listed items.

[00109] It should be understood that 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.”

[00110] The foregoing specification is only preferred embodiments of one or more embodiments of the present specification and 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, the method comprising:

selecting one or more blockchain assets from a remitter's blockchain account according to a transaction amount of a transaction to be remitted from the remitter's blockchain account into a receiver's blockchain account, wherein a total asset amount represented by the selected one or more blockchain assets is not less than the transaction amount, and a commitment of an individual asset amount represented by each of the selected one or more blockchain assets is recorded in a blockchain;

generating a commitment of the transaction amount; and

submitting to the blockchain the transaction comprising information of the selected one or more blockchain assets and the commitment of the transaction amount, for the selected one or more blockchain assets to be removed from the remitter's blockchain account and one or more blockchain assets corresponding to the commitment of the transaction amount to be added to the receiver's blockchain account,

wherein the commitment of the transaction amount is obtained by applying an encryption algorithm to the transaction amount and a transaction random number, and wherein the computing device is associated with the remitter, and the method further comprises:

before submitting the transaction to the blockchain, 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, according to the encryption algorithm and the transaction random number, a transaction asset amount represented by the one or more blockchain assets to be added to the receiver's blockchain account.

2. The method of claim 1, wherein the encryption algorithm is Pedersen Commitment.

3. The method of claim 1 or 2, before submitting the transaction to the blockchain, further comprising:

sending the commitment of the transaction amount to the computing device associated

with the receiver via an 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.

4. The method of claim 3, before submitting the transaction to the blockchain, further comprising:

obtaining a receiver signature generated by the computing device associated with the receiver based on a receiver private key after successfully verifying the association, wherein the receiver signature represents the receiver's endorsement for the commitment of the transaction amount; and

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

5. The method of any preceding claim, further comprising:

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

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

6. The method of any preceding claim, further comprising:

generating a range proof, wherein the range proof is related to the transaction amount; and

adding the range proof to the transaction.

7. The method of any preceding claim, before submitting the transaction to the blockchain, further comprising:

generating a commitment of a change amount in response to the total asset amount represented by the selected one or more blockchain assets being more than the transaction amount, wherein the change amount is a difference between the total asset amount of the

selected one or more blockchain assets and the transaction amount; and

adding the commitment of the change amount to the transaction, for one or more blockchain assets corresponding to the commitment of the change amount to be credited back to the remitter's blockchain account.

8. The method of claim 7, wherein:

the commitment of the individual asset amount (Mi) is obtained by applying a homomorphic encryption algorithm to the individual asset amount (pi) and an asset random number (ri), wherein $0<i\leqslant k$ and k is the number of the selected one or more blockchain assets;

the commitment of the transaction amount (T) is obtained by applying the homomorphic encryption algorithm to the transaction amount (t) and a transaction random number (r);

the commitment of the change amount (T0) is obtained by applying the homomorphic encryption algorithm to the change amount (t0) and a change random number (r0); and

before submitting the transaction to the blockchain, the method further comprises:

generating a verification random number (r'), wherein r'=r1+……+rk-r-r0; and

adding the verification random number (r') to the transaction for blockchain nodes in the blockchain to verify whether an input of the transaction is equal to an output of the transaction.

9. The method of claim 8, wherein the input of the transaction is verified to be equal to the output of the transaction in response to a verification commitment (R') corresponding to the verification random number r' is equal to M1+……+Mk-T-T0.

10. The method of claim 7, wherein the commitment of the change amount is obtained by applying the homomorphic encryption algorithm to the change amount and a change random number.

11. The method of claim 10, before submitting the transaction to the blockchain, further comprising:

generating a range proof, wherein the range proof is related to the change amount; and

adding the range proof to the transaction.

12. 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 the claims 1 to 11.

13. An apparatus for implementing blockchain-based transactions, comprising a plurality of modules for performing the method of any of the claims 1 to 11.

14. 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 the claims 1 to 11.