

BLOCKCHAIN-BASED CROSS-CURRENCY SETTLEMENT METHODS, APPARATUSES, AND ELECTRONIC DEVICES

TECHNICAL FIELD

One or more embodiments of this specification relate to the field of blockchain technologies, and in particular, to blockchain-based cross-currency settlement methods and apparatuses, and electronic devices.

BACKGROUND

Blockchain technology, also referred to as a distributed ledger technology, is an emerging technology in which a plurality of computer devices participate in “accounting” to jointly maintain a complete distributed database. Because the blockchain technology features decentralization, openness and transparency, allowing all the computer devices to participate in database recording, and quick data synchronization between the computer devices, the blockchain technology is widely applied to a variety of fields.

SUMMARY

This specification provides a blockchain-based cross-currency settlement method, applicable to a settlement system built based on a blockchain, where the settlement system includes a first settlement node inside a territory, a transit node, and a second settlement node outside the territory, the transit node opens a first settlement account at the first settlement node, and the transit node opens a second settlement account at the second settlement node, the method including:

creating, for the transit node in response to a determination that off-chain funds of a first currency transferred by the first settlement node to the first settlement account are in a frozen state, a first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain; and creating, for the transit node in response to a determination that off-chain funds of a second currency transferred by the second settlement node to the second settlement account are in a frozen state, a second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain;

receiving a fund exchange transaction sent by the transit node, where the fund exchange transaction is a transaction created by the transit node according to fund exchange instructions

from the first settlement node and the second settlement node; and

transferring, in response to the fund exchange transaction, the first blockchain asset from a blockchain account corresponding to the transit node to a blockchain account corresponding to the second settlement node and transferring the second blockchain asset from the blockchain account corresponding to the transit node to a blockchain account corresponding to the first settlement node, for the first settlement node or the second settlement node to perform a cross-currency fund settlement for a user based on the blockchain asset transferred to the respective blockchain account.

Optionally, the creating, for the transit node in response to a determination that off-chain funds of a first currency transferred by the first settlement node to the first settlement account are in a frozen state, a first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain includes:

receiving an asset creation transaction sent by the first settlement node, where the asset creation transaction includes a freeze credential of the off-chain funds of the first currency transferred by the first settlement node to the first settlement account; and

calling an asset creation logic in a smart contract published in the blockchain in response to the asset creation transaction, to create the first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain for the transit node based on the freeze credential, and adding the created first blockchain asset to the blockchain account corresponding to the transit node for holding.

Optionally, the creating, for the transit node in response to a determination that off-chain funds of a second currency transferred by the second settlement node to the second settlement account are in a frozen state, a second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain includes:

receiving an asset creation transaction sent by the second settlement node, where the asset creation transaction includes a freeze credential of the off-chain funds of the second currency transferred by the second settlement node to the second settlement account; and

calling an asset creation logic in a smart contract published in the blockchain in response to the asset creation transaction, to create the second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain for the transit node based on the freeze credential, and adding the created second blockchain asset to the blockchain account corresponding to the transit node for holding.

Optionally, the transferring, in response to the fund exchange transaction, the first blockchain asset from a blockchain account corresponding to the transit node to a blockchain

account corresponding to the second settlement node and transferring the second blockchain asset from the blockchain account corresponding to the transit node to a blockchain account corresponding to the first settlement node includes:

calling an asset exchange logic in a smart contract published in the blockchain in response to the fund exchange transaction, to transfer the first blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the second settlement node, and transfer the second blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the first settlement node.

Optionally, the method further includes:

receiving a fund settlement transaction sent by the first settlement node or the second settlement node, where the fund settlement transaction is a transaction created by the first settlement node or the second settlement node according to an instruction, sent by the user, of performing a cross-currency fund settlement according to a blockchain asset; and

calling an asset settlement logic in a smart contract published in the blockchain in response to the fund settlement transaction, to further transfer the blockchain asset held in the blockchain account corresponding to the first settlement node or the second settlement node to a blockchain account of the user for holding, to complete the cross-currency fund settlement.

Optionally, the method further includes:

receiving an asset conversion transaction sent by the first settlement node or the second settlement node, where the asset conversion transaction is a transaction created according to an instruction, sent by the user, of performing a cross-currency fund settlement based on off-chain funds; and

calling an asset conversion logic in a smart contract published in the blockchain in response to the asset conversion transaction, to mark the blockchain asset held in the blockchain account corresponding to the first settlement node or the second settlement node in a deregistered state, for a settlement node at a peer end of the first settlement node or the second settlement node to unfreeze off-chain funds corresponding to the blockchain asset in response to a determination that the blockchain asset is in a deregistered state, and transfer the unfrozen off-chain funds to a settlement account opened at the first settlement node or the second settlement node by the user.

Optionally, the method further includes:

receiving an asset conversion transaction sent by a user client, where the asset conversion transaction is a transaction created by the client according to an instruction, sent by the user, of

converting a held blockchain asset; and

calling the asset conversion logic in the smart contract published in the blockchain in response to the asset conversion transaction, to mark a blockchain asset held in a blockchain account of the user in a deregistered state, for the first settlement node or the second settlement node to unfreeze off-chain funds corresponding to the blockchain asset in response to a determination that the blockchain asset held in the blockchain account of the user is in a deregistered state, and transfer the unfrozen off-chain funds to the settlement account opened at the first settlement node or the second settlement node by the user.

Optionally, the settlement nodes are banks, the transit node is an intermediary bank, and the first settlement account and the second settlement account are nostro/vostro accounts.

Optionally, the transit node is a branch bank node of the first settlement node inside a territory in which the second settlement node is located, or the transit node is a branch bank node of the second settlement node inside the territory in which the first settlement node is located.

Optionally, the settlement nodes are banks, the transit node is a non-bank institution, and the first settlement account and the second settlement account are client reserve accounts opened at bank nodes by the non-bank institution.

Optionally, the user is a non-bank institution opening a client reserve account at the first settlement node or the second settlement node.

Optionally, the non-bank institution is a third-party payment institution.

Optionally, the non-bank institution is an issuing institution of a stored value instrument.

Optionally, the cross-currency fund settlement includes cross-currency remittance settlement.

Optionally, the cross-currency fund settlement includes cross-currency foreign exchange transaction settlement.

Optionally, the blockchain asset includes an on-chain balance issued on the blockchain based on frozen off-chain funds.

This specification further provides a blockchain-based cross-currency settlement apparatus, applicable to a settlement system built based on a blockchain, where the settlement system includes a first settlement node inside a territory, a transit node, and a second settlement node outside the territory, the transit node opens a first settlement account at the first settlement node, and the transit node opens a second settlement account at the second settlement node, the apparatus including:

a creation module, configured to create, for the transit node in response to a determination

that off-chain funds of a first currency transferred by the first settlement node to the first settlement account are in a frozen state, a first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain; and create, for the transit node in response to a determination that off-chain funds of a second currency transferred by the second settlement node to the second settlement account are in a frozen state, a second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain;

a receiving module, configured to receive a fund exchange transaction sent by the transit node, where the fund exchange transaction is a transaction created by the transit node according to fund exchange instructions from the first settlement node and the second settlement node; and

a transfer module, configured to transfer, in response to the fund exchange transaction, the first blockchain asset from a blockchain account corresponding to the transit node to a blockchain account corresponding to the second settlement node and transfer the second blockchain asset from the blockchain account corresponding to the transit node to a blockchain account corresponding to the first settlement node, for the first settlement node or the second settlement node to perform a cross-currency fund settlement for a user based on the blockchain asset transferred to the respective blockchain account.

Optionally, the creation module is configured to:

receive an asset creation transaction sent by the first settlement node, where the asset creation transaction includes a freeze credential of the off-chain funds of the first currency transferred by the first settlement node to the first settlement account; and

call an asset creation logic in a smart contract published in the blockchain in response to the asset creation transaction, to create the first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain for the transit node based on the freeze credential, and add the created first blockchain asset to the blockchain account corresponding to the transit node for holding.

Optionally, the creation module is configured to:

receive an asset creation transaction sent by the second settlement node, where the asset creation transaction includes a freeze credential of the off-chain funds of the second currency transferred by the second settlement node to the second settlement account; and

call an asset creation logic in a smart contract published in the blockchain in response to the asset creation transaction, to create the second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain for the transit node based on the freeze credential, and add the created second blockchain asset to the blockchain account

corresponding to the transit node for holding.

Optionally, the transfer module is configured to:

call an asset exchange logic in a smart contract published in the blockchain in response to the fund exchange transaction, to transfer the first blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the second settlement node, and transfer the second blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the first settlement node.

Optionally, the transfer module is further configured to:

receive a fund settlement transaction sent by the first settlement node or the second settlement node, where the fund settlement transaction is a transaction created by the first settlement node or the second settlement node according to an instruction, sent by the user, of performing a cross-currency fund settlement according to a blockchain asset; and

call an asset settlement logic in a smart contract published in the blockchain in response to the fund settlement transaction, to further transfer the blockchain asset held in the blockchain account corresponding to the first settlement node or the second settlement node to a blockchain account of the user for holding, to complete the cross-currency fund settlement.

Optionally, the apparatus further includes:

a conversion module, configured to receive an asset conversion transaction sent by the first settlement node or the second settlement node, where the asset conversion transaction is a transaction created according to an instruction, sent by the user, of performing a cross-currency fund settlement based on off-chain funds; and

call an asset conversion logic in a smart contract published in the blockchain in response to the asset conversion transaction, to mark the blockchain asset held in the blockchain account corresponding to the first settlement node or the second settlement node in a deregistered state, for a settlement node at a peer end of the first settlement node or the second settlement node to unfreeze off-chain funds corresponding to the blockchain asset in response to a determination that the blockchain asset is in a deregistered state, and transfer the unfrozen off-chain funds to a settlement account opened at the first settlement node or the second settlement node by the user.

Optionally, the conversion module is further configured to:

receive an asset conversion transaction sent by a user client, where the asset conversion transaction is a transaction created by the client according to an instruction, sent by the user, of converting a held blockchain asset; and

call the asset conversion logic in the smart contract published in the blockchain in response to the asset conversion transaction, to mark a blockchain asset held in a blockchain account of the user in a deregistered state, for the first settlement node or the second settlement node to unfreeze off-chain funds corresponding to the blockchain asset in response to a determination that the blockchain asset held in the blockchain account of the user is in a deregistered state, and transfer the unfrozen off-chain funds to the settlement account opened at the first settlement node or the second settlement node by the user.

Optionally, the settlement nodes are banks, the transit node is an intermediary bank, and the first settlement account and the second settlement account are nostro/vostro accounts.

Optionally, the transit node is a branch bank node of the first settlement node inside a territory in which the second settlement node is located, or the transit node is a branch bank node of the second settlement node inside the territory in which the first settlement node is located.

Optionally, the settlement nodes are banks, the transit node is a non-bank institution, and the first settlement account and the second settlement account are client reserve accounts opened at bank nodes by the non-bank institution.

Optionally, the user is a non-bank institution opening a client reserve account at the first settlement node or the second settlement node.

Optionally, the non-bank institution is a third-party payment institution.

Optionally, the non-bank institution is an issuing institution of a stored value instrument.

Optionally, the cross-currency fund settlement includes cross-currency remittance settlement.

Optionally, the cross-currency fund settlement includes cross-currency foreign exchange transaction settlement.

Optionally, the blockchain asset includes an on-chain balance issued on the blockchain based on frozen off-chain funds.

In the foregoing technical solutions, when cross-currency settlement nodes perform cross-currency settlement by using a transit node, after the first settlement node and the second settlement node respectively transfer off-chain funds of different currencies to the settlement accounts opened at the first settlement node and the second settlement node by the transit node, the off-chain funds in the settlement accounts can be frozen, and blockchain assets corresponding to the frozen off-chain funds in the settlement accounts are issued on the blockchain. Then a cross-currency fund exchange is completed based on the blockchain assets issued on the blockchain without directly using the off-chain funds. Therefore, a relatively long

fund delivery cycle caused by different system accounting time of bank nodes and the transit node in a cross-currency fund exchange directly using off-chain funds can be avoided, and the effectiveness of the cross-currency fund exchange can be significantly improved, to implement real-time settlement based on a blockchain asset.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram of creating a smart contract according to an exemplary embodiment;

FIG. 2 is a schematic diagram of calling a smart contract according to an exemplary embodiment;

FIG. 3 is a schematic diagram of creating and calling a smart contract according to an exemplary embodiment;

FIG. 4 is a schematic diagram of a blockchain-based settlement system according to an exemplary embodiment;

FIG. 5 is a flowchart of a blockchain-based settlement method according to an exemplary embodiment;

FIG. 6 is a schematic diagram of a cross-currency remittance settlement scenario according to an exemplary embodiment;

FIG. 7 is a schematic diagram of a cross-currency foreign exchange transaction settlement scenario according to an exemplary embodiment;

FIG. 8 is a schematic structural diagram of an electronic device according to an exemplary embodiment; and

FIG. 9 is a block diagram of a blockchain-based settlement apparatus according to an exemplary embodiment.

DETAILED DESCRIPTION

Exemplary embodiments are described in detail herein, and examples of the exemplary embodiments are shown in the accompanying drawings. When the following description involves the accompanying drawings, unless otherwise indicated, the same numerals in different accompanying drawings represent the same or similar elements. The implementations described in the following exemplary embodiments are not all the implementations consistent with one or more embodiments of this specification, but are instead only examples of methods and apparatuses that are described in detail in the appended claims and that are consistent with

some aspects of one or more embodiments of this specification.

It should be noted that in other embodiments, the steps of corresponding methods are not necessarily performed according to a sequence shown and described in this specification. In some other embodiments, the methods may include more or fewer steps than those described in this specification. In addition, a single step described in this specification may be divided into a plurality of steps for description in other embodiments, and a plurality of steps described in this specification may be combined into a single step for description in other embodiments.

Blockchains are generally classified into three types: a public blockchain, a private blockchain, and a consortium blockchain. In addition, there may also be a combination of the types, for example, a combination of a private blockchain + a consortium blockchain, or a combination of a consortium blockchain + a public blockchain.

The public blockchain has the highest degree of decentralization. For the public blockchain, such as Bitcoin and Ethereum, participants joining the public blockchain (also referred to as nodes in the blockchain) may read data records on the blockchain, participate in transactions, compete for accounting rights on a new block, and the like. Moreover, each node may freely join or exit the blockchain network and perform related operations.

The private blockchain is opposite thereto, whose write permission is controlled by an organization or an institution, and data read permission is specified by an organization. Briefly, the private blockchain may be a weakly centralized system with strict restrictions on nodes and a relatively small quantity of nodes. A blockchain of such a type is more suitable for internal use in a particular institution.

The consortium blockchain is a blockchain between the public blockchain and the private blockchain, and may achieve partial decentralization. Nodes in the consortium blockchain generally correspond to entities or organizations, and nodes join the blockchain network through authorization to form a stakeholder consortium and jointly maintain the running of the blockchain.

Based on basic characteristics of a blockchain, the blockchain generally includes a plurality of blocks. Timestamps corresponding to moments at which these blocks are created are respectively recorded in the blocks. All the blocks strictly follow the timestamps recorded in the blocks to form a time-ordered data chain.

For real data generated in the physical world, the data may be constructed in a standard transaction format supported by the blockchain, and then published to the blockchain. Node devices in the blockchain perform consensus processing on a received transaction. After a consensus is reached, a node device as an accounting node in the blockchain packages the

transaction into a block for persistent storage in the blockchain.

Consensus algorithms supported in the blockchain may include:

a first-type consensus algorithm, that is, a consensus algorithm in which node devices need to compete for accounting rights of each round of accounting cycle, for example, Proof of Work (PoW), Proof of Stake (PoS), or Delegated Proof of Stake (DPoS); and

a second-type consensus algorithm, that is, a consensus algorithm in which an accounting node is selected in advance for each round of accounting cycle (without competition for accounting rights), for example, Practical Byzantine Fault Tolerance (PBFT).

In a blockchain network using the first-type consensus algorithm, after receiving a transaction, node devices competing for accounting rights may execute the transaction. In the node devices competing for accounting rights, there may be one node device winning in a current round of competing for accounting rights, and becoming an accounting node. The accounting node may package the received transaction and another transaction together to generate a candidate block, and send the generated candidate block or a block header of the candidate block to another node device for a consensus.

In a blockchain network using the second-type consensus algorithm, a node device having accounting rights is agreed before a current round of accounting. Therefore, after receiving a transaction, if a node device is not the accounting node of the current round, the node device may send the transaction to the accounting node. The accounting node of the current round may execute the transaction when or before packaging the transaction and another transaction together to generate a candidate block. After generating the candidate block, the accounting node may send the generated candidate block or a block header of the candidate block to another node device for a consensus.

As described above, no matter which one of the foregoing consensus algorithms is used on the blockchain, the accounting node of the current round may package a received transaction to generate a candidate block, and send the generated candidate block or a block header of the candidate block to another node device for verification and a consensus. If verification succeeds after the another node device receives the candidate block or the block header of the candidate block, the candidate block may be used as the latest block and added to the end of the original blockchain, so as to complete an accounting process of the blockchain. When verifying the new block or the block header sent by the accounting node, the another node device may execute the transaction included in the block.

In the field of blockchains, the blockchains may be generally classified, according to accounting manners supported by the blockchains, into a blockchain using an unspent

transaction output (UTXO) model, such as Bitcoin, and a blockchain using an account-based model, such as Ethereum.

For the blockchain using the account-based model, an object supported on the blockchain is generally represented in the form of an account. For example, objects supported by Ethereum generally include two types: an external object and a contract object. Therefore, accounts supported by Ethereum are also classified into two types: an external account and a contract account. The external object generally is a user, and the external account is an account directly controlled by the user, also referred to as a user account. The contract object is generally a smart contract, and the contract account is an account that is created by a user by using an external account and that includes executable smart contract code.

Certainly, for some blockchain models (for example, AntChain) derived based on an architecture of the blockchain using the account-based model, account types supported by the blockchain may be further increased, which is not particularly limited in this specification.

For an account on the blockchain, an account state of the account generally is maintained by using a structure. After a transaction in a block is executed, a state of an account related to the transaction on the blockchain generally changes.

For the blockchain using the account-based model, a structure of an account generally includes fields such as Balance, Nonce, Code, and Storage. The field Balance is used for maintaining a current account balance of the account.

The field Nonce is used for maintaining a quantity of transactions of the account, and is a counter used for ensuring that each transaction can be processed only once, to effectively avoid a replay attack.

The field Code is used for maintaining contract code of the account. In a practical application, the field Code generally maintains only a hash value of the contract code. Therefore, the field Code is generally also referred to as a field Codehash.

The field Storage is used for maintaining stored content of the account (a field value is a null value by default). An independent storage space is generally allocated to a contract account to store to-be-stored content of the contract account. The independent storage space is generally referred to as account storage of the contract account.

The to-be-stored content of the contract account is generally constructed in a data structure of a Merkle Patricia Trie (MPT) to be stored in the independent storage space. The MPT constructed based on the to-be-stored content of the contract account is generally referred to as a storage tree. The field Storage generally maintains only a root node of the storage tree. In addition, the field Storage is generally referred to as a field StorageRoot.

For the external account, field values of both the field Code and the field Storage are null values.

In a practical application, any one of the public blockchain, the private blockchain, and the consortium blockchain may provide a function of a smart contract. A smart contract on a blockchain is a contract that may be triggered by a transaction to be executed on the blockchain. The smart contract may be defined in the form of code.

For example, a user is allowed to create and call some complex logic in an Ethereum network. Ethereum is a programmable blockchain, and a core of Ethereum is an Ethereum virtual machine (EVM). Each Ethereum node may run an EVM. The EVM is a Turing-complete virtual machine, which can be used to implement various complex logic. A smart contract published and called by a user in Ethereum is run on the EVM. In practice, the EVM directly runs virtual machine code (which is virtual machine bytecode, briefly referred to as "bytecode" in the following). Therefore, the smart contract deployed on the blockchain may be bytecode.

As shown in FIG. 1, after Bob sends a transaction including information for creating a smart contract to an Ethereum network, each node may execute the transaction in an EVM. In FIG. 1, a field From of the transaction is used for recording an address of an account that initiates the creation of the smart contract, contract code stored by a field value of a field Data of the transaction may be bytecode, and a field value of a field To of the transaction is a null account. When nodes reach a consensus through a consensus mechanism, the smart contract is created successfully, and a user subsequently may call the smart contract.

After the smart contract is created, a contract account corresponding to the smart contract appears on a blockchain and has a specific address. For example, "0x68e12cf284..." in each node in FIG. 1 represents the address of the created contract account. The field Code and the field Storage of the contract account are stored in the account storage of the contract account. Behavior of the smart contract is controlled by the contract code, and the account storage of the smart contract maintains a state of the contract. In other words, the smart contract enables a virtual account including contract code and account storage to be generated on the blockchain.

As described above, the field Data of the transaction including the information for creating the smart contract may store bytecode of the smart contract. The bytecode includes a string of bytes, and each byte may identify an operation. Considering development efficiency, readability, and other aspects, a developer may not directly write bytecode but select a high-level language to write smart contract code.

For example, the high-level language may be a language such as Solidity, Serpent, or a

Lisp-like language (LLL). The smart contract code written in a high-level language may be compiled by a compiler to generate bytecode that can be deployed on the blockchain. For example, contract code written in the solidity language is quite similar to a class in an object-oriented programming language. A variety of members may be declared in a contract, including a state variable, a function, a function modifier, an event, and the like. The state variable is a value permanently stored in the account storage field (Storage) of the smart contract and is used for maintaining a state of the contract.

As shown in FIG. 2, still using Ethereum as an example, after Bob sends a transaction including information for calling a smart contract to an Ethereum network, each node may execute the transaction in an EVM. In FIG. 2, a field From of the transaction is used for recording an address of an account that initiates the calling of the smart contract, a field To is used for recording an address of the called smart contract, and a field Data of the transaction is used for recording a method and a parameter for calling the smart contract. After the smart contract is called, an account state of a contract account may be changed. Subsequently, a client may check the account state of the contract account by using an accessed blockchain node (for example, a node 1 in FIG. 2).

The smart contract may be executed independently on each node in a blockchain network in a specified manner. All execution records and data are stored on a blockchain. Therefore, after such a transaction is executed, a transaction credential that cannot be tampered with and is impossible to be lost is stored on the blockchain.

FIG. 3 is a schematic diagram of creating and calling a smart contract. To create a smart contract in Ethereum, processes such as writing the smart contract, generating bytecode, and deploying the bytecode on a blockchain are needed. Calling a smart contract in Ethereum is to initiate a transaction that points to an address of the smart contract. An EVM of each node may execute the transaction separately, so that smart contract code is run in a distributed way in the virtual machine of each node in an Ethereum network.

In the blockchain using the account-based model, such as Ethereum, to implement a "value transfer" on the blockchain, a currency in the real world is generally allowed to be converted into a virtual token that can circulate on the blockchain.

In the field of blockchains, for some blockchain models (for example, AntChain) derived based on the architecture of the blockchain using the account-based model, the function of converting a currency in the real world into a virtual token that can circulate on a blockchain is generally not supported. Instead, in these blockchain models, currencies and some non-monetary physical assets in the real world may be converted into virtual assets that can circulate

on the blockchain.

It should be noted that, converting a currency or a non-monetary physical asset in the real world into a virtual asset on a blockchain is generally a process of “anchoring” the currency or the physical asset with a virtual asset on the blockchain as value support of the virtual asset, and generating, on the blockchain, a virtual asset that matches the value of the currency or the physical asset and can circulate between blockchain accounts on the blockchain.

During implementation, the account types supported by the blockchain may be increased (that is, objects supported by the blockchain are increased), to add an asset account (also referred to as an asset object) based on an existing account type supported by the blockchain. For example, an asset account may be further added based on an external account and a contract account supported by the blockchain. The added asset account is a virtual asset that uses a currency or a non-monetary physical asset in the real world as value support and can circulate freely between blockchain accounts.

For a user who accesses such a blockchain, in addition to completing the creation of a user account and a smart contract on the blockchain, the user may further create, on the blockchain, a virtual asset that matches the value of a currency or a non-monetary physical asset in the real world and circulates on the blockchain. For example, the user may convert held non-monetary physical assets such as real estate, stocks, a loan contract, notes, receivables, and the like into virtual assets with matched value to circulate on the blockchain.

An account state of the asset account may also be maintained by using a structure. Content included in the structure of the asset account may be the same as the content included in the structure of the account supported by the foregoing described blockchain using the account-based model, and certainly, the content may alternatively be designed autonomously based on a practical requirement.

In an implementation, for example, the content included in the structure of the asset account is the same as the content included in the structure of the account supported by the foregoing described blockchain using the account-based model. The structure of the asset account may also include the foregoing described fields such as Balance, Nonce, Code, and Storage.

It should be noted that, in the blockchain using the account-based model, the field Balance is generally used for maintaining a current account balance of an account. However, for a blockchain model derived based on the architecture of the blockchain using the account-based model, the blockchain model may not support the function of converting a currency in the real world into a virtual token that can circulate on a blockchain. Therefore, for such a blockchain,

the meaning of the field Balance may be extended, so that the field does not represent a “balance” of an account, but is used for maintaining address information of an asset account corresponding to a “virtual asset” held in the account. In a practical application, the field Balance may maintain address information of asset accounts corresponding to a plurality of “virtual assets.”

In this case, the external account, the contract account, and the asset account all can hold, by adding address information of an asset account corresponding to a “virtual asset” that needs to be held to the field Balance, the virtual asset. That is, in addition to the external account and the contract account, the asset account may also hold a virtual asset.

For the asset account, the field values of the field Nonce and the field Code may be null values (or may not be null values), and the field value of the field Storage may not be a full value. The field Storage may be used for maintaining an asset state of a “virtual asset” corresponding to the asset account. A specific manner of maintaining the asset state of the “virtual asset” corresponding to the asset account in the field Storage may be flexibly designed based on a requirement and is not detailed herein.

In the blockchain model derived based on the architecture of the blockchain using the account-based model, a user may create, on a blockchain by using the following implementation, a virtual asset that matches the value of a currency or a non-monetary physical asset in the real world.

In an implementation, transaction types supported by the blockchain may be increased, to add a transaction for creating a virtual asset. For example, transaction types supported by Ethereum generally include an ordinary transfer transaction, a transaction for creating a smart contract, and a transaction for calling a smart contract. Then, a transaction for creating a virtual asset may be added on top of the three types of transactions.

In this case, the user may publish, by using a client, a transaction for creating a virtual asset to a blockchain network. A node device in the blockchain executes the transaction in a local EVM to create a virtual asset for the user. When node devices reach a consensus through a consensus mechanism, the virtual asset is successfully created, and an asset account corresponding to the virtual asset appears on the blockchain and has a specific address.

In another implementation, a smart contract for creating a virtual asset may alternatively be deployed on the blockchain. The process of deploying the smart contract for creating a virtual asset is not repeated herein.

In this case, the user may publish, by using a client, a transaction for calling the smart contract to a blockchain network. A node device in the blockchain executes the transaction in

a local EVM and runs contract code related to the smart contract in the EVM to create a virtual asset for the user. When node devices reach a consensus through a consensus mechanism, the virtual asset is successfully created, and an asset account corresponding to the virtual asset appears on the blockchain and has a specific address.

Certainly, if some blockchain models derived based on an architecture of Ethereum also support the function of converting a currency in the real world into a virtual token that can circulate on a blockchain, some non-monetary physical assets in the real world may still be converted into virtual tokens that can circulate on the blockchain, so as to circulate on the blockchain, which is not detailed in this specification.

This specification is intended to provide a technical solution of performing, in a scenario in which cross-currency settlement is implemented between cross-currency settlement nodes by using a transit node, real-time cross-currency settlement based on a blockchain asset that is issued on a blockchain and corresponds to settlement funds in a settlement account opened at a settlement node by an intermediate node.

During implementation, a settlement system may be built based on a blockchain. The settlement system includes a first settlement node inside a territory, a transit node, and a second settlement node outside the territory. The transit node opens a first settlement account at the first settlement node, and the transit node opens a second settlement account at the second settlement node.

During a cross-currency fund settlement based on the settlement system, a node device in the blockchain may create, for the transit node in response to a determination that off-chain funds of a first currency transferred by the first settlement node to the first settlement account are in a frozen state, a first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain, and create, for the transit node in response to a determination that off-chain funds of a second currency transferred by the second settlement node to the second settlement account are in a frozen state, a second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain.

After the first blockchain asset and the second blockchain asset are created on the blockchain for the transit node, the transit node may create a fund exchange transaction according to fund exchange instructions from the first settlement node and the second settlement node, and publish the fund exchange transaction to the blockchain.

After receiving the fund exchange transaction, the node device in the blockchain may transfer, in response to the fund exchange transaction, the first blockchain asset from a blockchain account corresponding to the transit node to a blockchain account corresponding to

the second settlement node and transfer the second blockchain asset from the blockchain account corresponding to the transit node to a blockchain account corresponding to the first settlement node.

After the fund exchange process is completed, the first settlement node and the second settlement node may further perform a cross-currency fund settlement for users based on the blockchain assets transferred to the respective blockchain accounts.

In the foregoing technical solution, after the first settlement node and the second settlement node respectively transfer off-chain funds of different currencies to the settlement accounts opened at the first settlement node and the second settlement node by the transit node, the off-chain funds in the settlement accounts can be frozen, and blockchain assets corresponding to the frozen off-chain funds in the settlement accounts are issued on the blockchain. Then a cross-currency fund exchange is completed based on the blockchain assets issued on the blockchain without directly using the off-chain funds. Therefore, a relatively long fund delivery cycle caused by different system accounting time of bank nodes and the transit node in a cross-currency fund exchange directly using off-chain funds can be avoided, and the effectiveness of the cross-currency fund exchange can be significantly improved, to implement real-time settlement based on a blockchain asset.

Referring to FIG. 4, FIG. 4 is an architecture diagram of a settlement system built based on a blockchain in this specification.

The settlement system shown in FIG. 4 may include a first settlement node inside a territory, a transit node, and a second settlement node outside the territory.

The first settlement node, the transit node, and the second settlement node may be added to a blockchain network as node devices of the blockchain to jointly maintain a blockchain ledger. Certainly, in a practical application, the first settlement node, the transit node, and the second settlement node may not be added to the blockchain as node devices of the blockchain, but access the blockchain by maintaining a connection with a node device on the blockchain, and persistently store data generated thereof on the blockchain.

It should be noted that, the first settlement node and the second settlement node may be banks, and the transit node may be an intermediary bank, or a non-bank institution that serves as a transit node. The non-bank institution may include a third-party payment institution, an issuing institution of a stored value instrument, or the like, which is not limited in this specification. For example, the stored value instrument may be E-Money or a prepaid card.

When the transit node is an intermediary bank, the intermediary bank may be a branch bank of the first settlement node inside a territory in which the second settlement node is

located. The transit node may alternatively be a branch bank of the second settlement node inside the territory in which the first settlement node is located. This is not limited in this specification.

In the settlement system shown in FIG. 4, the transit node may open settlement accounts at the first settlement node and the second settlement node respectively. In this specification, the settlement account opened at the first settlement node by the transit node may be represented by a first settlement account, and the settlement account opened at the second settlement node by the transit node may be represented by a second settlement account.

It should be noted that, specific types of the settlement accounts respectively opened at the first settlement node and the second settlement node by the transit node are related to a node type of the transit node.

For example, when the transit node is an intermediary bank, the first settlement account and the second settlement account may include a nostro/vostro account, a bank reserve account, a trust account, and the like.

When the transit node is a non-bank institution, the first settlement account and the second settlement account may include client reserve accounts opened at bank nodes by the non-bank institution.

Based on the architecture of the settlement system shown in FIG. 4, the first settlement node located inside the territory and the second settlement node located outside the territory may perform a cross-currency fund settlement by using the transit node. For example, the cross-currency fund settlement may include cross-currency remittance settlement or cross-currency foreign exchange transaction settlement.

Referring to FIG. 5, FIG. 5 is a flowchart of a blockchain-based cross-currency settlement method according to an exemplary embodiment. The method is applied to a node device in a blockchain based on which the settlement system shown in FIG. 4 is built. The method includes the following steps:

Step 502: Creating, for the transit node in response to a determination that off-chain funds of a first currency transferred by the first settlement node to the first settlement account are in a frozen state, a first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain; and creating, for the transit node in response to a determination that off-chain funds of a second currency transferred by the second settlement node to the second settlement account are in a frozen state, a second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain.

Step 504: Receiving a fund exchange transaction sent by the transit node, where the fund

exchange transaction is a transaction created by the transit node according to fund exchange instructions from the first settlement node and the second settlement node.

Step 506: Transferring, in response to the fund exchange transaction, the first blockchain asset from a blockchain account corresponding to the transit node to a blockchain account corresponding to the second settlement node and transferring the second blockchain asset from the blockchain account corresponding to the transit node to a blockchain account corresponding to the first settlement node, for the first settlement node or the second settlement node to perform a cross-currency fund settlement for a user based on the blockchain asset transferred to the respective blockchain account.

The technical solutions of this specification are described in detail below by using an example in which both the first settlement node and the second settlement node are banks.

It should be noted that, both the first settlement node and the second settlement node being banks is merely exemplary. In a practical application, either of the first settlement node and the second settlement node may be a non-bank institution, for example, may be a third-party payment institution or an issuing institution of a stored value instrument. Examples are not listed or described in this specification one by one.

In this specification, when the first bank node located inside the territory (that is, the first settlement node) and the second bank node located outside the territory (that is, the second settlement node) do not accept counterparty risks of each other, a nostro/vostro account is generally not opened at each other to deposit any form of assets.

In this case, if the first bank node and the second bank node need to perform a cross-currency fund settlement, an intermediate node that respectively opens settlement accounts at the first bank node and the second bank node and whose counterparty risk is accepted by both the first bank node and the second bank node is generally needed.

The intermediate node may be an intermediary bank whose counterparty risk is accepted by both the first bank node and the second bank node, or may be a non-bank institution whose counterparty risk is accepted by both the first bank node and the second bank node, for example, may be a third-party payment institution or an issuing institution of a stored value instrument.

In an implementation, if the intermediate node is an intermediary bank, the settlement accounts respectively opened at the first bank node and the second bank node by the intermediate node may be nostro/vostro accounts. Because a nostro/vostro account is a basic account type supported by a global banking system, the use of the nostro/vostro accounts has the advantage of higher versatility.

Certainly, in a practical application, the settlement account may alternatively be a bank

reserve account, a trust account, or the like with slightly lower versatility than the nostro/vostro account.

Correspondingly, if the intermediate node is a non-bank institution, the settlement accounts respectively opened at the first bank node and the second bank node by the intermediate node may be client reserve accounts opened at the bank nodes by the non-bank institution. Because a client reserve account is also a basic account type supported by a global banking system, the use of the client reserve accounts also has the advantage of higher versatility.

In this specification, after the first bank node and the second bank node determine the intermediate node, the first bank node and the second bank node may complete the cross-currency fund settlement with each other by using the intermediate node whose counterparty risk is accepted as a fund transit.

For example, the first bank node may transfer to-be-settled off-chain funds of a first currency to the first settlement account opened at the first bank node by the intermediate node. Correspondingly, the second bank node may also transfer to-be-settled off-chain funds of a second currency to the second settlement account opened at the second bank node by the intermediate node. It should be noted that, the off-chain funds of the first currency and the off-chain funds of the second currency may be equivalent currencies converted according to an exchange rate.

After the first bank node and the second bank node respectively transfer the off-chain funds of the first currency and the off-chain funds of the second currency that need to be settled to the settlement accounts respectively opened at the first bank node and the second bank node by the intermediate node, the first bank node and the second bank node may respectively freeze the off-chain funds in the first settlement account and the off-chain funds in the second settlement account, and then issue blockchain assets corresponding to the frozen funds on the blockchain by using the frozen funds as value support.

A specific form of the blockchain asset is not particularly limited in this specification. The blockchain asset may be in the form of the asset object described above, or may use another form other than the asset account described above. For example, in an implementation, the blockchain asset may be an on-chain balance issued on the blockchain based on the frozen off-chain funds.

After determining that the off-chain funds in the first settlement account and the second settlement account are in a frozen state, a node device in the blockchain may create, for the transit node, a first blockchain asset corresponding to the off-chain funds of the first currency and a second blockchain asset corresponding to the off-chain funds of the second currency on

the blockchain.

In an implementation, a smart contract for managing a blockchain asset may be deployed on the blockchain. The process of deploying the smart contract on the blockchain is not repeated herein. An execution logic corresponding to contract code in the smart contract may include an asset creation logic, an asset exchange logic, an asset conversion logic, and the like.

After freezing the off-chain funds of the first currency transferred to the first settlement account, the first bank node may generate a freeze credential for the funds, construct an asset creation transaction including the freeze credential for the funds, and then publish the asset creation transaction to the blockchain. The asset creation transaction may be a smart contract calling transaction.

After a consensus is reached on the asset creation transaction, the node device in the blockchain may call the asset creation logic in the smart contract in response to the asset creation transaction to create the first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain for the transit node based on the freeze credential, and add the created first blockchain asset to the blockchain account corresponding to the transit node for holding.

For example, when the first blockchain asset is the asset account described above, address information of the asset account corresponding to the first blockchain asset may be added to a field Balance in a structure of the blockchain account corresponding to the transit node. When the first blockchain asset is an on-chain balance issued on the blockchain based on the frozen off-chain funds, an account balance that is maintained by the field Balance in the structure of the blockchain account corresponding to the transit node and corresponds to such a blockchain asset may be updated based on the on-chain balance.

Correspondingly, after freezing the off-chain funds of the second currency transferred to the second settlement account, the second bank node may also generate a freeze credential for the funds, construct an asset creation transaction including the freeze credential for the funds, and then publish the asset creation transaction to the blockchain. The asset creation transaction may also be a smart contract calling transaction.

After a consensus is reached on the asset creation transaction, the node device in the blockchain may call the asset creation logic in the smart contract in response to the asset creation transaction, to create the second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain for the transit node based on the freeze credential, and add the created second blockchain asset to the blockchain account corresponding to the transit node for holding.

In this specification, after the first bank node and the second bank node respectively freeze the off-chain funds in the first settlement account and the off-chain funds in the second settlement account, and issue blockchain assets corresponding to the frozen funds on the blockchain by using the frozen funds as value support, the first bank node and the second bank node may each send a fund exchange instruction to the intermediate node.

A specific form of the fund exchange instruction is not limited in this specification. For example, the fund exchange instruction may be an instruction or a command line that is supported by the intermediate node and used for triggering a fund exchange.

After determining that the fund exchange instructions from the first bank node and the second bank node are received, the intermediate node may create a fund exchange transaction according to the instructions, and then publish the fund exchange transaction to the blockchain. The fund exchange transaction may also be a smart contract calling transaction.

After a consensus is reached on the fund exchange transaction, the node device in the blockchain may call the asset exchange logic in the smart contract in response to the fund exchange transaction, to transfer the first blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the second bank node, and transfer the second blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the first bank node.

For example, when the blockchain asset is the asset account described above, the address information of the asset account corresponding to the first block chain asset may be deleted, where the address information of the asset account is maintained by the field Balance in the structure of the blockchain account corresponding to the transit node, and then the address information of the asset account corresponding to the first blockchain asset is added to a field Balance in a structure of the blockchain account corresponding to the second bank node. Correspondingly, address information of an asset account corresponding to the second blockchain asset may further be deleted, where the address information of the asset account is maintained by the field Balance in the structure of the blockchain account corresponding to the transit node, and then the address information of the asset account corresponding to the second blockchain asset is added to a field Balance in a structure of the blockchain account corresponding to the first bank node.

When the blockchain asset is the on-chain balance issued on the blockchain based on the frozen off-chain funds, an account balance corresponding to an asset type of the first blockchain asset may be deduced, where the account balance is maintained by the field Balance in the structure of the blockchain account corresponding to the transit node, and then the account

balance corresponding to the asset type of the first blockchain asset is added to an account balance corresponding to the asset type of the first blockchain asset that is maintained by the field Balance in the structure of the blockchain account corresponding to the second bank node. Correspondingly, an account balance corresponding to an asset type of the second blockchain asset may further be deducted, where the account balance is maintained by the field Balance in the structure of the blockchain account corresponding to the transit node, and then the account balance corresponding to the asset type of the second blockchain asset is added to an account balance corresponding to the asset type of the second blockchain asset that is maintained by the field Balance in the structure of the blockchain account corresponding to the first bank node.

In this specification, after the node device of the blockchain completes the asset exchange process described above, the first bank node and the second bank node may perform a cross-currency fund settlement for users based on the blockchain assets transferred to the respective blockchain accounts.

The user may be a natural person user opening a settlement account at the first bank node or the second bank node, or may be a non-bank institution opening a client reserve account at the first bank node or the second bank node, for example, may be a third-party payment institution or an issuing institution of a stored value instrument.

In this specification, when the first bank node and the second bank node perform a cross-currency fund settlement for respective users based on the blockchain assets transferred to the respective blockchain accounts, if the user accepts the cross-currency fund settlement based on the blockchain asset rather than the off-chain funds, the cross-currency fund settlement may be directly performed for the user based on the blockchain assets. In contrary, if the user accepts the cross-currency fund settlement based on the off-chain funds rather than the blockchain asset, after the blockchain asset is converted into off-chain funds, the cross-currency fund settlement may be performed for the user based on the converted off-chain funds.

The following provides a description by using an example in which the first bank node performs a cross-currency fund settlement for a user based on the blockchain asset transferred to the blockchain account of the first bank node.

In an implementation, assuming that the user accepts the cross-currency fund settlement based on the blockchain asset, the user may send an instruction of performing the cross-currency fund settlement based on the blockchain asset to the first bank node. A specific form of the instruction is not limited in this specification. For example, the instruction may be an instruction or a command line that is supported by the bank node and used for instructing to

perform the cross-currency fund settlement based on the blockchain asset.

After determining that the instruction, from the user, of performing the cross-currency fund settlement based on the blockchain asset is received, the first bank node may create a fund settlement transaction according to the instruction, and then publish the fund settlement transaction to the blockchain. The fund settlement transaction may also be a smart contract calling transaction.

After a consensus is reached on the fund settlement transaction, the node device in the blockchain may call the asset settlement logic in the smart contract in response to the fund settlement transaction, to further transfer the blockchain asset held in the blockchain account of the first bank node to a blockchain account of the user for holding in order to complete the cross-currency fund settlement.

In this way, when the user accepts the cross-currency fund settlement based on the blockchain asset, the cross-currency fund settlement may be performed by directly using the blockchain assets that are issued on the blockchain and correspond to the settlement funds in the settlement accounts opened at the first bank node and the second bank node by the intermediate node, to implement real-time settlement based on the blockchain assets.

In another implementation, assuming that the user accepts the cross-currency fund settlement based on the off-chain funds rather than the blockchain asset, the user may send an instruction of performing the cross-currency fund settlement based on the off-chain funds to the first bank node.

After determining that the instruction, from the user, of performing the cross-currency fund settlement based on the off-chain funds is received, the first bank node may create an asset conversion transaction according to the instruction, and then publish the asset conversion transaction to the blockchain. The asset conversion transaction may also be a smart contract calling transaction.

After a consensus is reached on the asset conversion transaction, the node device in the blockchain may call the asset conversion logic in the smart contract in response to the asset conversion transaction, to mark the blockchain asset held in the blockchain account of the first bank node in a deregistered state.

Because the blockchain asset held in the first bank node is an asset issued on the blockchain based on the off-chain assets frozen by the second bank node at a peer end of the first bank node as value support, the second bank node holds a liability corresponding to the blockchain asset. In this case, when determining that the blockchain asset held in the blockchain account of the first bank node at the peer end is marked in a deregistered state, the second bank node

may unfreeze the off-chain funds corresponding to the blockchain asset, and then transfer the unfrozen off-chain funds to a settlement account opened at the first bank node or the second bank node by the user.

For example, in an implementation, if the user also opens a settlement account at the second bank node at the peer end of the first bank node, the second bank node may preferentially transfer, through balance transfer of an internal ledger, the unfrozen funds to the settlement account opened at the second bank node by the user.

In this way, when the user does not accept the cross-currency fund settlement based on a blockchain asset, a bank node holding a liability of the blockchain asset may unfreeze off-chain funds corresponding to the blockchain asset by calling the smart contract, and then perform the cross-currency fund settlement for the user based on the unfrozen off-chain funds.

In this specification, if the user accepts the cross-currency fund settlement based on the blockchain asset, after the blockchain asset is transferred to the blockchain account of the user for holding, if the user needs to convert the held blockchain asset into off-chain funds, a conversion of the blockchain asset held in the blockchain account of the user into the off-chain funds may be initiated.

In an implementation, assuming that the user needs to convert the blockchain asset held in the blockchain account into the off-chain funds, the user may initiate an instruction of converting the held blockchain asset to a user client.

After receiving the instruction, initiated by the user, of converting the held blockchain asset, the user client may create an asset conversion transaction according to the instruction, and then publish the asset conversion transaction to the blockchain. The asset conversion transaction may also be a smart contract calling transaction.

After a consensus is reached on the asset conversion transaction, the node device in the blockchain may call the asset conversion logic in the smart contract in response to the asset conversion transaction, to mark the blockchain asset held in the blockchain account of the user in a deregistered state.

Because the blockchain asset held by the user is an asset issued on the blockchain based on the off-chain assets frozen by the second bank node at the peer end of the first bank node as value support, the second bank node holds a liability corresponding to the blockchain asset. In this case, when determining that the blockchain asset held in the blockchain account of the user is marked in a deregistered state, the second bank node may unfreeze off-chain funds corresponding to the blockchain asset, and then transfer the unfrozen off-chain funds to a settlement account opened at the first bank node or the second bank node by the user.

In the foregoing embodiment, descriptions are made by using an example in which the first bank node performs the cross-currency fund settlement for a user based on a blockchain asset transferred to a blockchain account of the first bank node. In a practical application, a process in which the second bank node performs a cross-currency fund settlement for a user based on a blockchain asset transferred to a blockchain account of the second bank node is similar to the foregoing described process and is not repeated in this specification.

It should be noted that, the cross-currency fund settlement described in the foregoing embodiment may include a cross-currency fund settlement in any scenario, which is not particularly limited in this specification. For example, the scenario may include a cross-currency remittance settlement scenario and a cross-currency foreign exchange transaction settlement scenario.

The technical solutions in this specification are described in detail below respectively with reference to the cross-currency remittance settlement scenario and the cross-currency foreign exchange transaction settlement scenario.

Referring to FIG. 6, FIG. 6 is a schematic diagram of a cross-currency remittance settlement scenario in this specification.

As shown in FIG. 6, a bank 1 is a Hong Kong headquarter of a multinational bank and is one of the main settlement banks for Hong Kong dollar (HKD). A bank 3 is a headquarter of a Chinese-funded bank in China and is one of the main settlement banks for Chinese Yuan (CNY). The bank 1 and the bank 3, as main market makers for HKD and CNY foreign exchange transactions, open foreign exchange transaction accounts between each other. However, because the bank 1 and the bank 3 do not accept counterparty risks of each other, nostro/vostro accounts are not opened between each other to deposit any assets.

A client 1 opens an HKD settlement account (current account) at the bank 1 and deposits funds of a corresponding currency of the client 1 in the account. A client 2 opens a CNY settlement account at the bank 3 and deposits funds of a corresponding currency of the client 2 in the account.

A bank 2 shown in FIG. 6 is a China branch of the bank 1 and serves as an intermediary bank in remittance settlement between the bank 1 and the bank 3.

The bank 2 and the bank 1 accept counterparty risks of each other, and therefore, the bank 2 opens an HKD nostro/vostro account (that is, a first settlement account) at the bank 1 and deposits an HKD asset.

The bank 2 and the bank 3 also accept counterparty risks of each other, and therefore, the bank 2 opens a CNY nostro/vostro account (that is, a second settlement account) at the bank 3

and deposits a CNY asset.

In a cross-currency remittance settlement scenario, assuming that the client 1 needs to make a payment in HKD, and the payment is converted into equivalent CNY according to an agreed exchange rate, so as to remit the payment to the CNY settlement account opened at the bank 3 by the client 2.

In this scenario, if an HKD balance deposited in the HKD settlement account opened at the bank 1 by the client 1 is sufficient, the bank 1 may deduct a corresponding HKD amount from the HKD settlement account of the client 1 according to a remittance amount from the client 1. After the deduction is successful, the bank 1 may deposit HKD corresponding to the remittance amount (that is, off-chain funds of a first currency) in the HKD settlement account opened at the bank 1 by the bank 2.

Correspondingly, the bank 1 may further prompt the bank 3 as a receiving bank to deposit CNY corresponding to the remittance amount (that is, off-chain funds of a second currency) according to the agreed exchange rate in the CNY settlement account opened at the bank 3 by the bank 2.

After the bank 1 deposits HKD corresponding to the remittance amount in the HKD settlement account opened at the bank 1 by the bank 2, the bank 1 may freeze the HKD funds, create an HKD on-chain balance (that is, a first blockchain asset) on a blockchain by using the frozen HKD funds as value support, and add the created HKD on-chain balance to a blockchain account of the bank 2 for holding. The specific process of creating the HKD on-chain balance is not described herein.

Correspondingly, after the bank 3 deposits CNY corresponding to the remittance amount in the CNY settlement account opened at the bank 3 by the bank 2, the bank 3 may also freeze the CNY funds, create an CNY on-chain balance (that is, a second blockchain asset) on the blockchain by using the frozen CNY funds as value support, and add the created CNY on-chain balance to the blockchain account of the bank 2 for holding. The specific process of creating the CNY on-chain balance is not described herein.

Further, after the foregoing processes are completed, the bank 1 and the bank 3 may each send a fund exchange instruction to the bank 2. After determining that the fund exchange instructions from the bank 1 and the bank 3 are received, the bank 2 may create a fund exchange transaction according to the instructions, and then publish the fund exchange transaction to the blockchain.

A node device in the blockchain may, in response to the fund exchange transaction, transfer the HKD on-chain balance held in the blockchain account corresponding to the bank 2 to a

blockchain account corresponding to the bank 3 and transfer the CNY on-chain balance held in the blockchain account corresponding to the bank 2 to a blockchain account corresponding to the bank 1.

After the node device in the blockchain completes the foregoing described asset exchange process, the bank 1 may further prompt the client 2 on whether to accept cross-currency remittance settlement based on the CNY on-chain balance. If the client 2 accepts cross-currency remittance settlement based on the CNY on-chain balance, the client 2 may send an instruction of performing cross-currency remittance settlement based on the CNY on-chain balance to the bank 1.

After determining that the instruction, from the client 2, of performing cross-currency remittance settlement based on the CNY on-chain balance is received, the bank 1 may create a fund settlement transaction according to the instruction, and then publish the fund settlement transaction to the blockchain.

The node device in the blockchain may transfer the CNY on-chain balance held in the blockchain account corresponding to the bank 2 to a blockchain account corresponding to the client 2 in real time in response to the fund settlement transaction, so as to convert the payment in HKD made by the client 1 into a payment in CNY according to the agreed exchange rate and remit the payment in CNY to the account of the client 2 in a cross-currency way.

In this way, a relatively long fund delivery cycle caused by different system accounting time of the bank 1, the bank 2, and the bank 3 in cross-currency remittance settlement directly using off-chain funds can be avoided, and the effectiveness of the cross-currency remittance settlement can be significantly improved, to implement real-time settlement based on an on-chain balance.

Certainly, if the client 2 does not accept cross-currency remittance settlement based on the on-chain balance, the bank 1 may initiate a conversion to the bank 3 to convert the CNY on-chain balance held in the blockchain account into off-chain CNY funds, and then transfer the converted CNY funds to the CNY settlement account opened at the bank 3 by the client 2. The specific process of converting the CNY on-chain balance into the off-chain CNY funds is not described herein.

Referring to FIG. 7, FIG. 7 is a schematic diagram of a cross-currency foreign exchange transaction settlement scenario in this specification.

As shown in FIG. 7, a bank 1 is a Hong Kong headquarter of a multinational bank and is one of the main settlement banks for HKD. A bank 3 is a headquarter of a Chinese-funded bank in China and is also one of the main settlement banks for CNY. The bank 1 and the bank 3, as

main market makers for HKD and CNY foreign exchange transactions, open foreign exchange transaction accounts between each other. However, because the bank 1 and the bank 3 do not accept counterparty risks of each other, nostro/vostro accounts are not opened between each other to deposit any assets.

A client 1 opens HKD and CNY settlement accounts at the bank 1 and deposits funds of corresponding currencies of the client 1 in the accounts. A bank 2 shown in FIG. 7 is a China branch of the bank 1 and serves as an intermediary bank in cross-currency foreign exchange transaction settlement between the bank 1 and the bank 3.

The bank 2 and the bank 1 accept counterparty risks of each other, and therefore, the bank 2 opens an HKD nostro/vostro account (that is, a first settlement account) at the bank 1 and deposits an HKD asset.

The bank 2 and the bank 3 also accept counterparty risks of each other, and therefore, the bank 2 opens a CNY nostro/vostro account (that is, a second settlement account) at the bank 3 and deposits a CNY asset.

In a cross-currency foreign exchange transaction settlement scenario, it is assumed that the client 1 makes, through the bank 1, a foreign exchange transaction of selling HKD/buying CNY. The delivery of the foreign exchange transaction requires the client 1 to first deposit sufficient HKD funds in the HKD settlement account opened at the bank 1 as a reserve account by the client 1, and then the bank 1 delivers equivalent CNY funds according to an agreed exchange rate to a CNY reserve account opened at the bank 1 by the client 1.

Assuming that the bank 1 does not have sufficient CNY funds to be delivered to the client 1, the bank 1 needs to make a square foreign exchange transaction, through the bank 3, of selling HKD/buying CNY. The delivery of the square foreign exchange requires the bank 1 to pay a corresponding amount of HKD to the bank 3, and requires the bank 3 to pay a corresponding amount of CNY to the bank 1.

In this scenario, when the client 1 deposits sufficient HKD funds in the HKD settlement account opened at the bank 1 and the bank 1 delivers equivalent CNY funds according to the agreed exchange rate to the client 1, assuming that the bank 1 does not have sufficient CNY funds to be delivered to the client 1, the bank 1 may deposit a sufficient amount of HKD corresponding to the amount of to-be-delivered CNY (that is, off-chain funds of a first currency) in the HKD settlement account opened at the bank 1 by the bank 2.

Correspondingly, the bank 1 may further prompt the bank 3 as a receiving bank to deposit CNY corresponding to the amount of to-be-delivered CNY (that is, off-chain funds of a second currency) according to the agreed exchange rate in the CNY settlement account opened at the

bank 3 by the bank 2.

After the bank 1 deposits HKD corresponding to the amount of to-be-delivered CNY in the HKD settlement account opened at the bank 1 by the bank 2, the bank 1 may freeze the HKD funds, create an HKD on-chain balance (that is, a first blockchain asset) on a blockchain by using the frozen HKD funds as value support, and add the created HKD on-chain balance to a blockchain account of the bank 2 for holding. The specific process of creating the HKD on-chain balance is not described herein.

Correspondingly, after the bank 3 deposits CNY corresponding to the amount of to-be-delivered CNY in the CNY settlement account opened at the bank 3 by the bank 2, the bank 3 may also freeze the CNY funds, create an CNY on-chain balance (that is, a second blockchain asset) on the blockchain by using the frozen CNY funds as value support, and add the created CNY on-chain balance to the blockchain account of the bank 2 for holding. The specific process of creating the CNY on-chain balance is not described herein.

Further, after the foregoing processes are completed, the bank 1 and the bank 3 may each send a fund exchange instruction to the bank 2. After determining that the fund exchange instructions from the bank 1 and the bank 3 are received, the bank 2 may create a fund exchange transaction according to the instructions, and then publish the fund exchange transaction to the blockchain.

A node device in the blockchain may, in response to the fund exchange transaction, transfer the HKD on-chain balance held in the blockchain account corresponding to the bank 2 to a blockchain account corresponding to the bank 3 and transfer the CNY on-chain balance held in the blockchain account corresponding to the bank 2 to a blockchain account corresponding to the bank 1.

After the node device in the blockchain completes the foregoing described asset exchange process, the bank 1 may further prompt the client 1 on whether to accept cross-currency foreign exchange delivery settlement based on the CNY on-chain balance. If the client 1 accepts cross-currency foreign exchange delivery settlement based on the CNY on-chain balance, the client 1 may send an instruction of performing cross-currency foreign exchange delivery settlement based on the CNY on-chain balance to the bank 1.

After determining that the instruction, from the client 2, of performing cross-currency foreign exchange delivery settlement based on the CNY on-chain balance is received, the bank 1 may create a fund settlement transaction according to the instruction, and then publish the fund settlement transaction to the blockchain.

The node device in the blockchain may transfer the CNY on-chain balance held in the

blockchain account corresponding to the bank 2 to a blockchain account corresponding to the client 1 in real time in response to the fund settlement transaction, so as to complete the foreign exchange delivery settlement for a user.

In this way, a relatively long fund delivery cycle caused by different system accounting time of the bank 1, the bank 2, and the bank 3 in cross-currency foreign exchange transaction settlement directly using off-chain funds can be avoided, and the effectiveness of the cross-currency foreign exchange transaction settlement can be significantly improved, to implement real-time settlement based on an on-chain balance.

Certainly, if the client 1 does not accept cross-currency foreign exchange delivery settlement based on the CNY on-chain balance, the bank 1 may initiate a conversion to the bank 3 to convert the CNY on-chain balance held in the blockchain account into off-chain CNY funds, and then transfer the converted CNY funds to the CNY settlement account opened at the bank 1 by the client 1. The specific process of converting the CNY on-chain balance into the off-chain CNY funds is not described herein.

Corresponding to the foregoing method embodiment, this specification further provides an embodiment of a blockchain-based cross-currency settlement apparatus.

This embodiment of the blockchain-based cross-currency settlement apparatus in this specification is applicable to an electronic device. The apparatus embodiment may be implemented by using software, hardware, or a combination of software and hardware. Using a software implementation as an example, as a logical apparatus, the apparatus is formed by reading corresponding computer program instructions from a non-volatile memory into an internal memory by a processor of an electronic device where the apparatus is located.

On a hardware level, as shown in FIG. 8, which is a hardware structural diagram of an electronic device in which a blockchain-based cross-currency settlement apparatus according to this specification is located, the electronic device in which the apparatus is located in an embodiment not only includes a processor, a memory, a network interface, and a non-transitory storage shown in FIG. 8, but generally may also include other hardware according to actual functions of the electronic device, which is not detailed herein.

FIG. 9 is a block diagram of a blockchain-based cross-currency settlement apparatus according to an exemplary embodiment of this specification.

Referring to FIG. 9, a blockchain-based cross-currency settlement apparatus 90 is applicable to a node device in a blockchain based on which a settlement system shown in FIG. 4 is built. The node device has a hardware structure shown in FIG. 8. The settlement system includes a first settlement node inside a territory, a transit node, and a second settlement node

outside the territory. The transit node opens a first settlement account at the first settlement node, and the transit node opens a second settlement account at the second settlement node. The apparatus 90 includes:

- a creation module 901, configured to create, for the transit node in response to a determination that off-chain funds of a first currency transferred by the first settlement node to the first settlement account are in a frozen state, a first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain; and create, for the transit node in response to a determination that off-chain funds of a second currency transferred by the second settlement node to the second settlement account are in a frozen state, a second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain for the transit node;

- a receiving module 902, configured to receive a fund exchange transaction sent by the transit node, where the fund exchange transaction is a transaction created by the transit node according to fund exchange instructions from the first settlement node and the second settlement node; and

- a transfer module 903, configured to transfer, in response to the fund exchange transaction, the first blockchain asset from a blockchain account corresponding to the transit node to a blockchain account corresponding to the second settlement node and transfer the second blockchain asset from the blockchain account corresponding to the transit node to a blockchain account corresponding to the first settlement node, for the first settlement node or the second settlement node to perform a cross-currency fund settlement for a user based on the blockchain asset transferred to the respective blockchain account.

In this embodiment, the creation module 901 is configured to:

- receive an asset creation transaction sent by the first settlement node, where the asset creation transaction includes a freeze credential of the off-chain funds of the first currency transferred by the first settlement node to the first settlement account; and

- call an asset creation logic in a smart contract published in the blockchain in response to the asset creation transaction, to create the first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain for the transit node based on the freeze credential, and add the created first blockchain asset to the blockchain account corresponding to the transit node for holding.

In this embodiment, the creation module 901 is configured to:

- receive an asset creation transaction sent by the second settlement node, where the asset creation transaction includes a freeze credential of the off-chain funds of the second currency

transferred by the second settlement node to the second settlement account; and

call an asset creation logic in a smart contract published in the blockchain in response to the asset creation transaction, to create the second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain for the transit node based on the freeze credential, and add the created second blockchain asset to the blockchain account corresponding to the transit node for holding.

In this embodiment, the transfer module 903 is configured to:

call an asset exchange logic in a smart contract published in the blockchain in response to the fund exchange transaction, to transfer the first blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the second settlement node, and transfer the second blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the first settlement node.

In this embodiment, the transfer module is further configured to:

receive a fund settlement transaction sent by the first settlement node or the second settlement node, where the fund settlement transaction is a transaction created by the first settlement node or the second settlement node according to an instruction, sent by the user, of performing a cross-currency fund settlement according to a blockchain asset; and

call an asset settlement logic in a smart contract published in the blockchain in response to the fund settlement transaction, to further transfer the blockchain asset held in the blockchain account corresponding to the first settlement node or the second settlement node to a blockchain account of the user for holding, to complete the cross-currency fund settlement.

In this embodiment, the apparatus further includes:

a conversion module 904 (not shown in FIG. 9), configured to receive an asset conversion transaction sent by the first settlement node or the second settlement node, where the asset conversion transaction is a transaction created according to an instruction, sent by the user, of performing a cross-currency fund settlement based on off-chain funds; and

call an asset conversion logic in a smart contract published in the blockchain in response to the asset conversion transaction, to mark the blockchain asset held in the blockchain account corresponding to the first settlement node or the second settlement node in a deregistered state, for a settlement node at a peer end of the first settlement node or the second settlement node to unfreeze off-chain funds corresponding to the blockchain asset in response to a determination that the blockchain asset is in a deregistered state, and transfer the unfrozen off-chain funds to a settlement account opened at the first settlement node or the second settlement node by the

user.

In this embodiment, the conversion module is further configured to:

receive an asset conversion transaction sent by a user client, where the asset conversion transaction is a transaction created by the client according to an instruction, sent by the user, of converting a held blockchain asset; and

call the asset conversion logic in the smart contract published in the blockchain in response to the asset conversion transaction, to mark a blockchain asset held in a blockchain account of the user in a deregistered state, for the first settlement node or the second settlement node to unfreeze off-chain funds corresponding to the blockchain asset in response to a determination that the blockchain asset held in the blockchain account of the user is in a deregistered state, and transfer the unfrozen off-chain funds to the settlement account opened at the first settlement node or the second settlement node by the user.

In this embodiment, the settlement nodes are banks, the transit node is an intermediary bank, and the first settlement account and the second settlement account are nostro/vostro accounts.

In this embodiment, the transit node is a branch bank node of the first settlement node inside a territory in which the second settlement node is located, or the transit node is a branch bank node of the second settlement node inside the territory in which the first settlement node is located.

In this embodiment, the settlement nodes are banks, the transit node is a non-bank institution, and the first settlement account and the second settlement account are client reserve accounts opened at bank nodes by the non-bank institution.

In this embodiment, the user is a non-bank institution opening a client reserve account at the first settlement node or the second settlement node.

In this embodiment, the non-bank institution is a third-party payment institution.

In this embodiment, the non-bank institution is an issuing institution of a stored value instrument.

In this embodiment, the cross-currency fund settlement includes cross-currency remittance settlement.

In this embodiment, the cross-currency fund settlement includes cross-currency foreign exchange transaction settlement.

In this embodiment, the blockchain asset includes an on-chain balance issued on the blockchain based on frozen off-chain funds.

The system, the apparatus, the module, or the unit described in the foregoing embodiments

may be implemented by a computer chip or an entity, or implemented by a product having a certain function. A typical implementation device is a computer. A specific form of the computer may be a personal computer, a laptop computer, a cellular phone, a camera phone, a smartphone, a personal digital assistant, a media player, a navigation device, an email transceiver device, a game console, a tablet computer, a wearable device, or a combination of any devices of these devices.

In a typical configuration, the computer includes one or more processors (such as CPUs), an input/output interface, a network interface, and a memory.

The memory may include a form such as a volatile memory, a random access memory (RAM) and/or a non-volatile memory such as a read-only memory (ROM) or a flash RAM in a computer-readable medium. The memory is an example of the computer readable medium.

The computer-readable medium includes a non-volatile medium and a volatile medium, a removable medium and a non-removable medium, which may implement storage of information by using any method or technology. The information may be a computer-readable instruction, a data structure, a program module, or other data. Examples of a storage medium of a computer include, but are not limited to, a phase-change memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), a RAM of another type, a random access memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or another optical storage device, a cassette tape, a magnetic disk storage, a quantum memory, a graphene-based storage medium or another magnetic storage device, or any other non-transmission medium, which may be configured to store information accessible by a computer device. According to limitations of this specification, the computer-readable medium does not include transitory computer-readable media, such as a modulated data signal and a modulated carrier.

It should be further noted that, the term "include," "comprise," or any other variants are intended to cover a non-exclusive inclusion, so that a process, a method, a commodity, or a device that includes a series of elements not only includes such elements, but also includes other elements not expressly listed, or further includes elements inherent to such a process, method, commodity, or device. Unless otherwise specified, an element limited by "include a/an..." does not exclude other same elements existing in the process, the method, the article, or the device that includes the element.

Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps recorded in the

claims may be performed in sequences different from those in the embodiments and an expected result may still be achieved. In addition, the processes depicted in the accompanying drawings is not necessarily performed in the specific order or successively to achieve an expected result. In some implementations, multitasking and parallel processing may be feasible or beneficial.

The terms used in one or more embodiments of this specification are merely used to describe the embodiments but are not intended to limit one or more embodiments of this specification. The “a” and “the” in a singular form used in one or more embodiments of this specification and the appended claims are also intended to include a plural form, unless other meanings are clearly indicated in the context. It should be further understood that the term “and/or” used herein indicates and includes any or all possible combinations of one or more associated listed items.

It should be understood that although the terms “first,” “second,” “third,” and the like may be used to describe various information in one or more embodiments of this specification, such information should not be limited to these terms. These terms are merely used to distinguish between information of the same type. For example, without departing from the scope of one or more embodiments of this specification, first information may also be referred to as second information. Similarly, second information may also be referred to as first information. Depending on the context, for example, the word “if” used herein may be interpreted as “while” or “when,” or “in response to determination.”

The foregoing descriptions are merely exemplary embodiments of one or more embodiments of this specification, but are not intended to limit the one or more embodiments of this specification. Any modification, equivalent replacement, or improvement made within the spirit and principle of one or more embodiments of this specification shall fall within the protection scope of the one or more embodiments of this specification.

CLAIMS

What is claimed is:

1. A blockchain-based cross-currency settlement method, applicable to a settlement system built based on a blockchain, wherein the settlement system comprises a first settlement node inside a territory, a transit node, and a second settlement node outside the territory, the transit node opens a first settlement account at the first settlement node, and the transit node opens a second settlement account at the second settlement node, the method comprising:

creating, for the transit node in response to a determination that off-chain funds of a first currency transferred by the first settlement node to the first settlement account are in a frozen state, a first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain; and creating, for the transit node in response to a determination that off-chain funds of a second currency transferred by the second settlement node to the second settlement account are in a frozen state, a second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain;

receiving a fund exchange transaction sent by the transit node, wherein the fund exchange transaction is a transaction created by the transit node according to fund exchange instructions from the first settlement node and the second settlement node; and

transferring, in response to the fund exchange transaction, the first blockchain asset from a blockchain account corresponding to the transit node to a blockchain account corresponding to the second settlement node and transferring the second blockchain asset from the blockchain account corresponding to the transit node to a blockchain account corresponding to the first settlement node, for the first settlement node or the second settlement node to perform a cross-currency fund settlement for a user based on the blockchain asset transferred to the respective blockchain account.

2. The method according to claim 1, wherein the creating, for the transit node in response to a determination that off-chain funds of a first currency transferred by the first settlement node to the first settlement account are in a frozen state, a first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain comprises:

receiving an asset creation transaction sent by the first settlement node, wherein the asset creation transaction comprises a freeze credential of the off-chain funds of the first currency transferred by the first settlement node to the first settlement account; and

calling an asset creation logic in a smart contract published in the blockchain in response to the asset creation transaction, to create the first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain for the transit node based on the freeze credential, and adding the created first blockchain asset to the blockchain account corresponding to the transit node for holding.

3. The method according to claim 1, wherein the creating, for the transit node in response to a determination that off-chain funds of a second currency transferred by the second settlement node to the second settlement account are in a frozen state, a second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain comprises:

receiving an asset creation transaction sent by the second settlement node, wherein the asset creation transaction comprises a freeze credential of the off-chain funds of the second currency transferred by the second settlement node to the second settlement account; and

calling an asset creation logic in a smart contract published in the blockchain in response to the asset creation transaction, to create the second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain for the transit node based on the freeze credential, and adding the created second blockchain asset to the blockchain account corresponding to the transit node for holding.

4. The method according to claim 1, wherein the transferring, in response to the fund exchange transaction, the first blockchain asset from a blockchain account corresponding to the transit node to a blockchain account corresponding to the second settlement node and transferring the second blockchain asset from the blockchain account corresponding to the transit node to a blockchain account corresponding to the first settlement node comprises:

calling an asset exchange logic in a smart contract published in the blockchain in response to the fund exchange transaction, to transfer the first blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the second settlement node, and transfer the second blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the first settlement node.

5. The method according to claim 1, further comprising:

receiving a fund settlement transaction sent by the first settlement node or the second settlement node, wherein the fund settlement transaction is a transaction created by the first settlement node or the second settlement node according to an instruction, sent by the user, of performing a cross-currency fund settlement according to a blockchain asset; and

calling an asset settlement logic in a smart contract published in the blockchain in response to the fund settlement transaction, to further transfer the blockchain asset held in the blockchain account corresponding to the first settlement node or the second settlement node to a blockchain account of the user for holding, to complete the cross-currency fund settlement.

6. The method according to claim 1, further comprising:

receiving an asset conversion transaction sent by the first settlement node or the second settlement node, wherein the asset conversion transaction is a transaction created according to an instruction, sent by the user, of performing a cross-currency fund settlement based on off-chain funds; and

calling an asset conversion logic in a smart contract published in the blockchain in response to the asset conversion transaction, to mark the blockchain asset held in the blockchain account corresponding to the first settlement node or the second settlement node in a deregistered state, for a settlement node at a peer end of the first settlement node or the second settlement node to unfreeze off-chain funds corresponding to the blockchain asset in response to a determination that the blockchain asset is in a deregistered state, and transfer the unfrozen off-chain funds to a settlement account opened at the first settlement node or the second settlement node by the user.

7. The method according to claim 6, further comprising:

receiving an asset conversion transaction sent by a user client, wherein the asset conversion transaction is a transaction created by the client according to an instruction, sent by the user, of converting a held blockchain asset; and

calling the asset conversion logic in the smart contract published in the blockchain in response to the asset conversion transaction, to mark a blockchain asset held in a blockchain account of the user in a deregistered state, for the first settlement node or the second settlement node to unfreeze off-chain funds corresponding to the blockchain asset in response to a determination that the blockchain asset held in the blockchain account of the user is in a deregistered state, and transfer the unfrozen off-chain funds to the settlement account opened at the first settlement node or the second settlement node by the user.

8. The method according to claim 1, wherein the settlement nodes are banks, the transit node is an intermediary bank, and the first settlement account and the second settlement account are nostro/vostro accounts.

9. The method according to claim 8, wherein the transit node is a branch bank node of the first settlement node inside a territory in which the second settlement node is located, or the transit node is a branch bank node of the second settlement node inside the territory in which

the first settlement node is located.

10. The method according to claim 1, wherein the settlement nodes are banks, the transit node is a non-bank institution, and the first settlement account and the second settlement account are client reserve accounts opened at bank nodes by the non-bank institution.

11. The method according to claim 1, wherein the user is a non-bank institution opening a client reserve account at the first settlement node or the second settlement node.

12. The method according to claim 1, wherein the non-bank institution is a third-party payment institution.

13. The method according to claim 1, wherein the non-bank institution is an issuing institution of a stored value instrument.

14. The method according to claim 1, wherein the cross-currency fund settlement comprises cross-currency remittance settlement.

15. The method according to claim 1, wherein the cross-currency fund settlement comprises cross-currency foreign exchange transaction settlement.

16. The method according to claim 1, wherein the blockchain asset comprises an on-chain balance issued on the blockchain based on the frozen off-chain funds.

17. A blockchain-based cross-currency settlement apparatus, applicable to a settlement system built based on a blockchain, wherein the settlement system comprises a first settlement node inside a territory, a transit node, and a second settlement node outside the territory, the transit node opens a first settlement account at the first settlement node, and the transit node opens a second settlement account at the second settlement node, the apparatus comprising:

a creation module, configured to create, for the transit node in response to a determination that off-chain funds of a first currency transferred by the first settlement node to the first settlement account are in a frozen state, a first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain; and create, for the transit node in response to a determination that off-chain funds of a second currency transferred by the second settlement node to the second settlement account are in a frozen state, a second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain;

a receiving module, configured to receive a fund exchange transaction sent by the transit node, wherein the fund exchange transaction is a transaction created by the transit node according to fund exchange instructions from the first settlement node and the second settlement node; and

a transfer module, configured to transfer, in response to the fund exchange transaction, the first blockchain asset from a blockchain account corresponding to the transit node to a blockchain account corresponding to the second settlement node and transfer the second blockchain asset from the blockchain account corresponding to the transit node to a blockchain account corresponding to the first settlement node, for the first settlement node or the second settlement node to perform a cross-currency fund settlement for a user based on the blockchain asset transferred to the respective blockchain account.

18. The apparatus according to claim 17, wherein the creation module is configured to: receive an asset creation transaction sent by the first settlement node, wherein the asset creation transaction comprises a freeze credential of the off-chain funds of the first currency transferred by the first settlement node to the first settlement account; and

call an asset creation logic in a smart contract published in the blockchain in response to the asset creation transaction, to create the first blockchain asset corresponding to the off-chain funds of the first currency in the blockchain for the transit node based on the freeze credential, and add the created first blockchain asset to the blockchain account corresponding to the transit node for holding.

19. The apparatus according to claim 17, wherein the creation module is configured to: receive an asset creation transaction sent by the second settlement node, wherein the asset

creation transaction comprises a freeze credential of the off-chain funds of the second currency transferred by the second settlement node to the second settlement account; and

call an asset creation logic in a smart contract published in the blockchain in response to the asset creation transaction, to create the second blockchain asset corresponding to the off-chain funds of the second currency in the blockchain for the transit node based on the freeze credential, and add the created second blockchain asset to the blockchain account corresponding to the transit node for holding.

20. The apparatus according to claim 17, wherein the transfer module is configured to:

call an asset exchange logic in a smart contract published in the blockchain in response to the fund exchange transaction, to transfer the first blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the second settlement node, and transfer the second blockchain asset held in the blockchain account corresponding to the transit node to the blockchain account corresponding to the first settlement node.

21. The apparatus according to claim 17, wherein the transfer module is further configured to:

receive a fund settlement transaction sent by the first settlement node or the second settlement node, wherein the fund settlement transaction is a transaction created by the first settlement node or the second settlement node according to an instruction, sent by the user, of performing a cross-currency fund settlement according to a blockchain asset; and

call an asset settlement logic in a smart contract published in the blockchain in response to the fund settlement transaction, to further transfer the blockchain asset held in the blockchain account corresponding to the first settlement node or the second settlement node to a blockchain account of the user for holding, to complete the cross-currency fund settlement.

22. The apparatus according to claim 17, further comprising:

a conversion module, configured to receive an asset conversion transaction sent by the first settlement node or the second settlement node, wherein the asset conversion transaction is a transaction created according to an instruction, sent by the user, of performing a cross-currency fund settlement based on off-chain funds; and

call an asset conversion logic in a smart contract published in the blockchain in response to the asset conversion transaction, to mark the blockchain asset held in the blockchain account corresponding to the first settlement node or the second settlement node in a deregistered state, for a settlement node at a peer end of the first settlement node or the second settlement node to unfreeze off-chain funds corresponding to the blockchain asset in response to a determination that the blockchain asset is in a deregistered state, and transfer the unfrozen off-chain funds to a settlement account opened at the first settlement node or the second settlement node by the user.

23. The apparatus according to claim 22, wherein the conversion module is further configured to:

receive an asset conversion transaction sent by a user client, wherein the asset conversion transaction is a transaction created by the client according to an instruction, sent by the user, of converting a held blockchain asset; and

call the asset conversion logic in the smart contract published in the blockchain in response to the asset conversion transaction, to mark a blockchain asset held in a blockchain account of the user in a deregistered state, for the first settlement node or the second settlement node to unfreeze off-chain funds corresponding to the blockchain asset in response to a determination that the blockchain asset held in the blockchain account of the user is in a deregistered state, and transfer the unfrozen off-chain funds to the settlement account opened at the first settlement node or the second settlement node by the user.

24. The apparatus according to claim 17, wherein the settlement nodes are banks, the

transit node is an intermediary bank, and the first settlement account and the second settlement account are nostro/vostro accounts.

25. The apparatus according to claim 24, wherein the transit node is a branch bank node of the first settlement node inside a territory in which the second settlement node is located, or the transit node is a branch bank node of the second settlement node inside the territory in which the first settlement node is located.

26. The apparatus according to claim 17, wherein the settlement nodes are banks, the transit node is a non-bank institution, and the first settlement account and the second settlement account are client reserve accounts opened at bank nodes by the non-bank institution.

27. The apparatus according to claim 17, wherein the user is a non-bank institution opening a client reserve account at the first settlement node or the second settlement node.

28. The apparatus according to claim 17, wherein the non-bank institution is a third-party payment institution.

29. The apparatus according to claim 17, wherein the non-bank institution is an issuing institution of a stored value instrument.

30. The apparatus according to claim 17, wherein the cross-currency fund settlement comprises cross-currency remittance settlement.

31. The apparatus according to claim 17, wherein the cross-currency fund settlement comprises cross-currency foreign exchange transaction settlement.

32. The apparatus according to claim 17, wherein the blockchain asset comprises an on-chain balance issued on the blockchain based on the frozen off-chain funds.

33. An electronic device, comprising:
a processor; and
a memory configured to store instructions executable by the processor,
wherein the processor executes the executable instructions to implement the method according to any one of claims 1 to 16.

34. A computer-readable storage medium, storing computer instructions, wherein the instructions, when executed by a processor, implement steps of the method according to any one of claims 1 to 16.