

TRANSACTION METHOD AND SYSTEM BASED ON CENTRALIZED SETTLEMENT AND BLOCK CHAIN STORAGE

TECHNICAL FIELD

[0001] Embodiments of this specification relate to the field of information technologies, and in particular, to a transaction method and system based on centralized settlement and blockchain attestation.

BACKGROUND

[0002] Currently, the main mode of online electronic transaction is that a centralized settlement platform (such as a bank or Alipay) is responsible for managing an account of a user, transactions between users are executed and recorded by using the settlement platform, and the users may query the settlement platform for income and expenditure records of the accounts of the users for verification.

[0003] However, the income and expenditure records of the user accounts stored in the settlement platform may be tampered with, and therefore cannot be used as a trusted account reconciliation credential.

SUMMARY

[0004] To resolve the problem of untrusted income and expenditure records of a user account stored in a centralized settlement platform, embodiments of this specification provide a transaction method and system based on centralized settlement and blockchain attestation, and the technical solutions are as follows:

[0005] According to a first aspect of the embodiments of this specification, a transaction method based on centralized settlement and blockchain attestation is provided, where a blockchain network includes a plurality of member nodes, a virtual resource account is registered by a user with a designated member node, and the method includes:

[0006] receiving, by the designated member node, a transaction request including a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount;

[0007] performing transaction feasibility verification according to the transaction request,

and performing an account balance modification operation after the verification is successful, the account balance modification operation being deducting the designated resource amount from a virtual resource account corresponding to the paying user identifier and adding the designated resource amount to a virtual resource account corresponding to the receiving user identifier; and

[0008] generating a log file used for recording the account balance modification operation, and broadcasting the log file to the blockchain network, for the member nodes to publish the log file to a blockchain based on a consensus mechanism.

[0009] According to a second aspect of the embodiments of this specification, a transaction apparatus based on centralized settlement and blockchain attestation is provided, where a blockchain network includes a plurality of member nodes, a virtual resource account is registered by a user with a designated member node, and the apparatus includes:

[0010] a receiving module, configured to receive a transaction request including a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount;

[0011] a settlement module, configured to perform transaction feasibility verification according to the transaction request, and perform an account balance modification operation after the verification is successful, the account balance modification operation being deducting the designated resource amount from a virtual resource account corresponding to the paying user identifier and adding the designated resource amount to a virtual resource account corresponding to the receiving user identifier; and

[0012] an attestation module, configured to generate a log file used for recording the account balance modification operation, and broadcast the log file to the blockchain network, for the member nodes to publish the log file to a blockchain based on a consensus mechanism.

[0013] According to a third aspect of the embodiments of this specification, a transaction system based on centralized settlement and blockchain attestation is provided, where the system includes a blockchain network formed by a plurality of member nodes, and a user can register a virtual resource account with a designated member node, where

[0014] the designated member node receives a transaction request including a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount; performs transaction

feasibility verification according to the transaction request, and performs an account balance modification operation after the verification is successful, the account balance modification operation being deducting the designated resource amount from a virtual resource account corresponding to the paying user identifier and adding the designated resource amount to a virtual resource account corresponding to the receiving user identifier; and generates a log file used for recording the account balance modification operation, and broadcasts the log file to the blockchain network; and

[0015] other member nodes and the designated member node publish the log file to a blockchain based on a consensus mechanism.

[0016] In the technical solutions provided in the embodiments of this specification, a blockchain network includes a plurality of member nodes, and a virtual resource account is registered by a user with a designated member node. When receiving a transaction request, the designated member node performs transaction feasibility verification according to the transaction request, and performs an account balance modification operation after the verification is successful. That is, the designated resource amount is deducted from a virtual resource account corresponding to the paying user identifier, and the designated resource amount is added to a virtual resource account corresponding to the receiving user identifier. Moreover, the designated member node further generates a log file used for recording the account balance modification operation, and broadcasts the log file to the blockchain network, for the member nodes to publish the log file to a blockchain based on a consensus mechanism. In other words, for a transaction, a log file generated when the designated member node performs transaction settlement is published to the blockchain for attestation, which is equivalent to publishing income and expenditure records of a user account stored in a centralized settlement platform to the blockchain for attestation. Therefore, the income and expenditure records of the user account are difficult to be tampered with, and may be used as a trusted account reconciliation credential.

[0017] It should be understood that the foregoing general description and detailed description in the following are merely exemplary and explanative, and cannot constitute a limitation to the embodiments of this specification.

[0018] In addition, any one of the embodiments of this specification does not need to achieve all the foregoing effects.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] To describe the technical solutions in the embodiments of this specification or in the existing technologies more clearly, the following briefly describes the accompanying drawings required for describing the embodiments or the existing technologies. Apparently, the accompanying drawings in the following description show merely some of the embodiments of this specification, and a person of ordinary skill in the art may still derive other drawings from the accompanying drawings.

[0020] FIG. 1 is a schematic flowchart of a transaction method based on centralized settlement and blockchain attestation, according to an embodiment of this specification;

[0021] FIG. 2a is an exemplary flowchart of a transaction method based on centralized settlement and blockchain attestation, according to an embodiment of this specification;

[0022] FIG. 2b is an exemplary flowchart of another transaction method based on centralized settlement and blockchain attestation, according to an embodiment of this specification;

[0023] FIG. 2c is an exemplary flowchart of another transaction method based on centralized settlement and blockchain attestation, according to an embodiment of this specification;

[0024] FIG. 3 is a schematic flowchart of another transaction method based on centralized settlement and blockchain attestation, according to an embodiment of this specification;

[0025] FIG. 4 is a schematic flowchart of another transaction method based on centralized settlement and blockchain attestation, according to an embodiment of this specification;

[0026] FIG. 5 is a schematic structural diagram of a transaction apparatus based on centralized settlement and blockchain attestation, according to an embodiment of this specification;

[0027] FIG. 6 is a schematic structural diagram of a transaction device based on centralized settlement and blockchain attestation, according to an embodiment of this specification;

[0028] FIG. 7 is a schematic structural diagram of another transaction device based on centralized settlement and blockchain attestation, according to an embodiment of this specification;

[0029] FIG. 8 is a schematic structural diagram of a transaction system based on centralized settlement and blockchain attestation, according to an embodiment of this specification;

[0030] FIG. 9 is a schematic structural diagram of another transaction system based on centralized settlement and blockchain attestation, according to an embodiment of this

specification;

[0031] FIG. 10 is a schematic structural diagram of another transaction system based on centralized settlement and blockchain attestation, according to an embodiment of this specification; and

[0032] FIG. 11 is a schematic structural diagram of a computer device configured for the method shown in FIG. 1.

DETAILED DESCRIPTION

[0033] To enable a person skilled in the art to better understand technical solutions in the embodiments of this specification, the technical solutions in the embodiments of this specification are described in detail below with reference to the accompanying drawings in the embodiments of this specification. Obviously, the described embodiments are only a part of the embodiments of this specification, other than all of the embodiments. Based on the embodiments in this specification, all other embodiments obtained by a person of ordinary skill in the art should fall within the protection scope.

[0034] The technical solutions provided in the embodiments of this specification are described in detail below with reference to the accompanying drawings.

[0035] FIG. 1 is a schematic flowchart of another transaction method based on centralized settlement and blockchain attestation, according to an embodiment of this specification. The method includes the following steps:

[0036] S100. A designated member node receives a transaction request including a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user.

[0037] In this embodiment of this specification, a blockchain network includes a plurality of member nodes. It should be noted that, in this specification, a “node” may be one or more devices managed by a management party (a person or an institution), and management parties to which the member nodes respectively correspond are usually different.

[0038] In this embodiment of this specification, a virtual resource account is registered by a user with the designated member node. The designated member node may be designated according to actual service needs. For example, assuming that the blockchain network is a consortium blockchain network formed by 10 financial institutions (including banks and electronic payment platforms), a member node managed by an electronic payment platform may be designated as a designated member node, and a virtual resource account is registered

by a user with the electronic payment platform.

[0039] It should be noted that, the virtual resource account registered by the user with the designated member node is actually maintained in a relational database of the designated member node.

[0040] It should be further noted that, a virtual resource described in this specification is not limited to an electronic currency, and may be further a bonus point, a game currency, a virtual object, and the like. In short, a transaction may be performed between users by using any virtual resource as a transaction medium according to actual service rules.

[0041] In step S100, the designated member node may receive a transaction request sent by the paying user, or may receive a transaction request sent by the receiving user. The transaction request usually includes a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount.

[0042] S102. Perform transaction feasibility verification according to the transaction request, and perform an account balance modification operation after the verification is successful.

[0043] In this specification, the transaction feasibility verification refers to verifying whether a transaction is reasonable and executable, which mainly includes verifying whether an account balance of the paying user is sufficient. In addition, in practice, other items of the transaction may also be the subject of feasibility verification according to actual service rules, for example, whether the paying user has authorization. If the verification is successful, it indicates that the transaction is reasonable and executable.

[0044] If feasibility verification performed by the designated member node according to the transaction request is successful, an account balance modification operation is performed. That is, the designated resource amount is deducted from a virtual resource account corresponding to the paying user identifier, and the designated resource amount is added to a virtual resource account corresponding to the receiving user identifier.

[0045] S104. Generate a log file used for recording the account balance modification operation, and broadcast the log file to the blockchain network.

[0046] In step S104, the designated member node may generate a log file used for recording the account balance modification operation. It should be noted herein that, the log file is a record file or a file set used for recording an operation event of a software system (such as a windows system, a service logic processing system, and a database management

system). A suffix of the log file is generally .log.

[0047] After generating the log file, the designated member node may broadcast the log file to the blockchain network, for the member nodes to publish the log file to a blockchain based on a consensus mechanism.

[0048] It should be noted herein that, the blockchain network does not need to verify the feasibility of the transaction request according to the log file, provided that the member nodes publish the log file to the blockchain based on the consensus mechanism.

[0049] It should be further noted that, in this embodiment of this specification, an execution sequence of step S102 and step S104 is not limited. Step S104 may be performed after step S102 is performed, or step S102 may be performed after step S104 is performed, or step S102 and step S104 may be performed at the same time.

[0050] Through the transaction method based on centralized settlement and blockchain attestation shown in FIG. 1, for a transaction, a log file generated when the designated member node performs transaction settlement is published to a blockchain for attestation, which is equivalent to publishing income and expenditure records of a user account stored in a centralized settlement platform to the blockchain for attestation. Therefore, the income and expenditure records of the user account are difficult to be tampered with, and may be used as a trusted account reconciliation credential.

[0051] FIG. 2a is an exemplary flowchart of a transaction method based on centralized settlement and blockchain attestation, according to an embodiment of this specification. As shown in FIG. 2a, a blockchain network is formed by a plurality of member nodes (6 member nodes are shown in the figure). A solid circle is a designated member node, and hollow circles are member nodes other than the designated member node. A paying user may initiate a transaction, and send a transaction request to the designated member node. The designated member node first locally performs an account balance modification operation, generates a log file for recording the account balance modification operation, and then broadcasts the log file to the whole network, for the member nodes to publish the log file to the blockchain at the member nodes. It is worth emphasizing that, the designated member node needs to perform feasibility verification on the transaction, but the blockchain network does not need to perform feasibility verification on the transaction.

[0052] In addition, in this embodiment of this specification, the designated member node may generate a log file summary corresponding to the log file according to the log file by using a hash algorithm, and then broadcast the log file and the log file summary to the blockchain network, for the member nodes to publish the log file and the log file summary to

the blockchain based on a consensus mechanism.

[0053] In addition, the designated member node may send the log file summary to the paying user and/or the receiving user, for the paying user and/or the receiving user to query the blockchain for the log file by using the log file summary.

[0054] It is well-known that, for a piece of information, a summary (a string) of the piece of information may be obtained by performing a hash operation, and may uniquely identify the piece of information. Therefore, the log file summary may be used as an identifier of the log file. After the log file summary is provided to the paying user and/or the receiving user, the paying user or the receiving user can query the blockchain for the log file by using the log file summary as a clue, to determine that the designated member node has performed the account balance modification operation.

[0055] In practice, after broadcast to the member nodes, the log file is respectively stored into caches (or referred to as transaction pools) of the member nodes. When a designated consensus trigger condition is met (for example, after a designated period), a member node is selected from the member nodes based on a consensus mechanism to retrieve several log files and corresponding log file summaries from a transaction pool. The member node packs the log files and the log file summaries into a block, and broadcasts the block to the whole network, for the member nodes to respectively publish the block to the blockchain. In this way, the foregoing log file and log file summary are attested.

[0056] Therefore, in this embodiment of this specification, the designated member node may further send the log file summary to the paying user and/or the receiving user after it is determined that the log file is published to the blockchain.

[0057] In this case, when the paying user and/or the receiving user receive the log file summary sent by the designated member node, it means that the transaction is successful. If the paying user and/or the receiving user does not receive the log file summary, even if the designated member node has performed the account balance modification operation, it does not mean that the transaction is successful (because the log file has not been published to the blockchain).

[0058] In addition, the designated member node may alternatively send the log file summary to the paying user and/or the receiving user after it is determined that the log file is packed into a block.

[0059] In addition, the designated member node may include a service logic execution module, a database management module, and a blockchain function module.

[0060] The service logic execution module is responsible for outward interfacing with a

user, and processing a service according to a service request of the user. The service logic execution module may usually be software installed on the designated member node, or may be a hardware component of the designated member node.

[0061] The database management module is responsible for managing a local database of the designated member node, for example, modifying data in the database. The database management module may usually be software installed on the designated member node, or may be a hardware component of the designated member node.

[0062] The blockchain function module is an interface through which the designated member node accesses to the blockchain network, and may usually be software installed on the designated member node, or may be a hardware component of the designated member node.

[0063] In this way, in step S100, the designated member node may receive the transaction request by using the service logic execution module. In step S102, the designated member node performs the transaction feasibility verification according to the transaction request by using the service logic execution module, and performs the account balance modification operation by using the database management module if the verification is successful.

[0064] In step S104, the designated member node may generate the log file by using the service logic execution module (referring to FIG. 2b), or may generate the log file by using the database management module (referring to FIG. 2c). Next, the designated member node may broadcast the log file to the blockchain network by using the blockchain function module, and then publish the log file to a blockchain at the designated member node by using the blockchain function module.

[0065] FIG. 3 is a schematic flowchart of another transaction method based on centralized settlement and blockchain attestation, according to an embodiment of this specification. The method includes the following steps:

[0066] S300. A service logic execution module receives a transaction request including a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user.

[0067] In the method shown in FIG. 3, a blockchain network includes a plurality of member nodes, a virtual resource account is registered by a user with a designated member node, and the designated member node includes the service logic execution module, a database management module, and a blockchain function module.

[0068] S302. The service logic execution module performs transaction feasibility verification according to the transaction request, and sends an account balance modification

instruction to the database management module after the verification is successful.

[0069] S304. The database management module performs an account balance modification operation in a database according to the account balance modification instruction.

[0070] In the method shown in FIG. 3, the service logic execution module is responsible for accepting the transaction request and performing the transaction feasibility verification. After the verification is successful, the service logic execution module may instruct the database management module to perform the account balance modification operation. That is, the designated resource amount is deducted from a virtual resource account corresponding to the paying user identifier, and the designated resource amount is added to a virtual resource account corresponding to the receiving user identifier.

[0071] S306. The service logic execution module generates a log file used for recording the account balance modification operation, and sends the log file to the blockchain function module.

[0072] In the method shown in FIG. 3, the service logic execution module is responsible for generating the log file and sending the generated log file to the blockchain function module.

[0073] For example, a log file generating logic may be written into the service logic execution module in advance, and is performed by the service logic execution module. The log file generating logic may not only include a logic for recording the account balance modification operation, but also may include a logic for recording other transaction-related information (e.g., a transaction time point, a transaction location, a transaction postscript, etc.).

[0074] In the method shown in FIG. 3, after performing the account balance modification operation, the database management module may return a modification success notification to the service logic execution module. After receiving the modification success notification, the service logic execution module may generate the log file used for recording the account balance modification operation.

[0075] S308. The blockchain function module broadcasts the log file to the blockchain network, for the member nodes to publish the log file to a blockchain based on a consensus mechanism.

[0076] In step S308, the blockchain function module is responsible for broadcasting the log file to the blockchain network.

[0077] In addition, in step S308, the blockchain function module may, for example, generate a log file summary corresponding to the log file according to the log file by using a

hash algorithm, and then broadcast the log file and the log file summary to the blockchain network, for the member nodes to publish the log file and the log file summary to the blockchain based on the consensus mechanism.

[0078] The blockchain function module may send the log file summary to the service logic execution module. Then, the service logic execution module sends the log file summary to the paying user and/or the receiving user, for the paying user and/or the receiving user to query the blockchain for the log file by using the log file summary.

[0079] Further, the blockchain function module sends the log file summary to the service logic execution module if it is determined that the log file is published to the blockchain.

[0080] For the method shown in FIG. 3, it should be noted that, the service logic execution module is responsible for generating the log file. No complicated reconstruction needs to be performed on the service logic execution module, and only the log file generating logic needs to be written into the service logic execution module. In addition, the service logic execution module is responsible for generating the log file, and may also customize the content of the log file. In this way, the log file is not only used for recording the account balance modification operation, but also may be used for recording other transaction-related information.

[0081] FIG. 4 is a schematic flowchart of another transaction method based on centralized settlement and blockchain attestation, according to an embodiment of this specification. The method includes the following steps:

[0082] S400. A service logic execution module receives a transaction request including a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user.

[0083] In the method shown in FIG. 4, a blockchain network includes a plurality of member nodes, a virtual resource account is registered by a user with a designated member node, and the designated member node includes the service logic execution module, a database management module, and a blockchain function module.

[0084] S402. The service logic execution module performs transaction feasibility verification according to the transaction request, and sends an account balance modification instruction to the database management module after the verification is successful.

[0085] S404. The database management module performs an account balance modification operation according to the account balance modification instruction, and generates a log file used for recording the account balance modification operation.

[0086] In the method shown in FIG. 4, the service logic execution module is responsible

for accepting the transaction request and performing the transaction feasibility verification. After the verification is successful, the service logic execution module may instruct the database management module to perform the account balance modification operation. That is, the designated resource amount is deducted from a virtual resource account corresponding to the paying user identifier, and the designated resource amount is added to a virtual resource account corresponding to the receiving user identifier.

[0087] In the method shown in FIG. 4, the database management module is responsible for generating the log file and sending the generated log file to the blockchain function module.

[0088] It is well known to a person skilled in the art that, to ensure atomicity of a transaction, when performing data modification on a database, the database management module generally first generates a database log recording a data modification operation, and then performs the data modification operation according to the database log.

[0089] It can be seen that, in the method shown in FIG. 4, the log file is the database log. Moreover, the database management module may generate the log file before performing the account balance modification operation.

[0090] S406. The database management module sends the log file to the blockchain function module.

[0091] S408. The blockchain function module broadcasts the log file to the blockchain network.

[0092] In step S408, the blockchain function module generates a log file summary corresponding to the log file according to the log file by using a hash algorithm, and then broadcasts the log file and the log file summary to the blockchain network, for the member nodes to publish the log file and the log file summary to a blockchain based on a consensus mechanism.

[0093] The blockchain function module may send the log file summary to the database management module. Then, the database management module sends the log file summary to the service logic execution module, and the service logic execution module sends the log file summary to the paying user and/or the receiving user, for the paying user and/or the receiving user to query the blockchain for the log file by using the log file summary.

[0094] Further, the blockchain function module sends the log file summary to the database management module if it is determined that the log file is published to the blockchain. In addition, the designated member node may alternatively send the log file summary to the paying user and/or the receiving user after it is determined that the log file is packed into a block.

[0095] In addition, it should be noted that, the database management module may return, in a timely manner, a modification success notification to the service logic execution module after performing the account balance modification operation. Alternatively, the database management module may not return a modification success notification temporarily after performing the account balance modification operation, but return the modification success notification and the log file summary together to the service logic execution module after receiving the log file summary returned by the blockchain function module.

[0096] Based on the transaction method based on centralized settlement and blockchain attestation shown in FIG. 1, an embodiment of this specification further correspondingly provides a transaction apparatus based on centralized settlement and blockchain attestation. As shown in FIG. 5, a blockchain network includes a plurality of member nodes, the apparatus is any of the member nodes, a virtual resource account is registered by a user with the apparatus, and the apparatus includes:

[0097] a receiving module 501, configured to receive a transaction request including a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount;

[0098] a settlement module 502, configured to perform transaction feasibility verification according to the transaction request, and perform an account balance modification operation after the verification is successful, the account balance modification operation being deducting the designated resource amount from a virtual resource account corresponding to the paying user identifier and adding the designated resource amount to a virtual resource account corresponding to the receiving user identifier; and

[0099] an attestation module 503, configured to generate a log file used for recording the account balance modification operation, and broadcast the log file to the blockchain network, for the member nodes to publish the log file to a blockchain based on a consensus mechanism.

[0100] The attestation module 503 generates a log file summary corresponding to the log file according to the log file by using a hash algorithm, and then broadcasts the log file and the log file summary to the blockchain network, for the member nodes to publish the log file and the log file summary to the blockchain based on the consensus mechanism.

[0101] The apparatus further includes: a sending module 504, configured to send the log file summary to the paying user and/or the receiving user, for the paying user and/or the receiving user to query the blockchain for the log file by using the log file summary.

[0102] The sending module 504 sends the log file summary to the paying user and/or the receiving user if it is determined that the log file is published to the blockchain.

[0103] Based on the transaction method based on centralized settlement and blockchain attestation shown in FIG. 3, an embodiment of this specification further correspondingly provides a transaction device based on centralized settlement and blockchain attestation. As shown in FIG. 6, a blockchain network includes a plurality of member nodes, the device is any of the member nodes, a virtual resource account is registered by a user with the device, and the device includes a service logic execution module 601, a database management module 602, and a blockchain function module 603.

[0104] The service logic execution module 601 receives a transaction request including a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount; performs transaction feasibility verification according to the transaction request, and sends an account balance modification instruction to the database management module after the verification is successful; and generates a log file used for recording an account balance modification operation, and sends the log file to the blockchain function module, the account balance modification operation being deducting the designated resource amount from a virtual resource account corresponding to the paying user identifier and adding the designated resource amount to a virtual resource account corresponding to the receiving user identifier.

[0105] The database management module 602 performs the account balance modification operation according to the account balance modification instruction.

[0106] The blockchain function module 603 broadcasts the log file to the blockchain network, for the member nodes to publish the log file to a blockchain based on a consensus mechanism.

[0107] The service logic execution module 601 generates the log file used for recording the account balance modification operation and recording other transaction-related information.

[0108] After performing the account balance modification operation, the database management module 602 returns a modification success notification to the service logic execution module.

[0109] After receiving the modification success notification, the service logic execution module 601 generates the log file used for recording the account balance modification operation.

[0110] The blockchain function module 603 generates a log file summary corresponding to the log file according to the log file by using a hash algorithm; broadcasts the log file and the log file summary to the blockchain network, for the member nodes to publish the log file and the log file summary to the blockchain based on the consensus mechanism; and sends the log file summary to the service logic execution module.

[0111] The service logic execution module 601 sends the log file summary to the paying user and/or the receiving user, for the paying user and/or the receiving user to query the blockchain for the log file by using the log file summary.

[0112] The blockchain function module 603 sends the log file summary to the service logic execution module if it is determined that the log file is published to the blockchain.

[0113] Based on the transaction method based on centralized settlement and blockchain attestation shown in FIG. 4, an embodiment of this specification further correspondingly provides a transaction device based on centralized settlement and blockchain attestation. As shown in FIG. 7, a blockchain network includes a plurality of member nodes, the device is any of the member nodes, a virtual resource account is registered by a user with the device, and the device includes a service logic execution module 701, a database management module 702, and a blockchain function module 703.

[0114] The service logic execution module 701 receives a transaction request including a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount; and performs transaction feasibility verification according to the transaction request, and sends an account balance modification instruction to the database management module after the verification is successful.

[0115] The database management module 702 performs an account balance modification operation according to the account balance modification instruction, and generates a log file used for recording the account balance modification operation, the account balance modification operation being deducting the designated resource amount from a virtual resource account corresponding to the paying user identifier and adding the designated resource amount to a virtual resource account corresponding to the receiving user identifier; and sends the log file to the blockchain function module.

[0116] The blockchain function module 703 broadcasts the log file to the blockchain network, for the member nodes to publish the log file to a blockchain based on a consensus mechanism.

[0117] The blockchain function module 703 generates a log file summary corresponding to the log file according to the log file by using a hash algorithm; broadcasts the log file and the log file summary to the blockchain network, for the member nodes to publish the log file and the log file summary to the blockchain based on the consensus mechanism; and sends the log file summary to the database management module.

[0118] The database management module 702 sends the log file summary to the service logic execution module.

[0119] The service logic execution module 701 sends the log file summary to the paying user and/or the receiving user, for the paying user and/or the receiving user to query the blockchain for the log file by using the log file summary.

[0120] The blockchain function module 703 sends the log file summary to the database management module if it is determined that the log file is published to the blockchain.

[0121] The database management module 702 sends the log file summary and a modification success notification together to the service logic execution module.

[0122] FIG. 8 is a schematic structural diagram of a transaction system based on centralized settlement and blockchain attestation, according to an embodiment of this specification. The system includes a blockchain network formed by a plurality of member nodes, where a user can register a virtual resource account with a designated member node.

[0123] The designated member node receives a transaction request including a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount; performs transaction feasibility verification according to the transaction request, and performs an account balance modification operation after the verification is successful, the account balance modification operation being deducting the designated resource amount from a virtual resource account corresponding to the paying user identifier and adding the designated resource amount to a virtual resource account corresponding to the receiving user identifier; and generates a log file used for recording the account balance modification operation, and broadcasts the log file to the blockchain network.

[0124] Other member nodes and the designated member node publish the log file to a blockchain based on a consensus mechanism.

[0125] The designated member node generates a log file summary corresponding to the log file according to the log file by using a hash algorithm; broadcasts the log file and the log file summary to the blockchain network, for the member nodes to publish the log file and the log

file summary to the blockchain based on the consensus mechanism; and sends the log file summary to the paying user and/or the receiving user, for the paying user and/or the receiving user to query the blockchain for the log file by using the log file summary.

[0126] The designated member node sends the log file summary to the paying user and/or the receiving user if it is determined that the log file is published to the blockchain.

[0127] FIG. 9 is a schematic structural diagram of another transaction system based on centralized settlement and blockchain attestation, according to an embodiment of this specification. The system includes a blockchain network formed by a plurality of member nodes, where each member node includes the device shown in FIG. 6, and a virtual resource account is registered by a user with the device.

[0128] FIG. 10 is a schematic structural diagram of another transaction system based on centralized settlement and blockchain attestation, according to an embodiment of this specification. The system includes a blockchain network formed by a plurality of member nodes, where each member node includes the device shown in FIG. 7, and a virtual resource account is registered by a user with the device.

[0129] An embodiment of this specification further provides a computer device, where a blockchain network includes a plurality of member nodes, the device is any of the member nodes, and a virtual resource account is registered by a user with the device.

[0130] The device includes at least a memory, a processor, and a computer program stored on the memory and executable on the processor. When executing the program, the processor implements functions of the method shown in FIG. 1.

[0131] FIG. 11 is a schematic diagram of a more detailed hardware structure of a computer device, according to an embodiment of this specification. The device may include: a processor 1110, a memory 1120, an input/output interface 1130, a communication interface 1140, and a bus 1150. The processor 1110, the memory 1120, the input/output interface 1130, and the communication interface 1140 communicate with and connect to each other inside the device by using the bus 1150.

[0132] The processor 1110 may be implemented in a manner of a general central processing unit (CPU), a microprocessor, an application-specific integrated circuit (ASIC), or one or more integrated circuits, and is configured to execute a related program to implement the technical solutions provided in the embodiments of this specification.

[0133] The memory 1120 may be implemented in a form of a read-only memory (ROM), a random access memory (RAM), a static storage device, or a dynamic storage device. The memory 1120 may store an operating system and another application program. When the

technical solutions provided in the embodiments of this specification are implemented by means of software or firmware, related program code is stored in the memory 1120 and is executed by the processor 1110.

[0134] The input/output interface 1130 is configured to connect to an input/output module, to implement input and output of information. The input/output module may be used as a component and configured in the device (not shown in the figure), or may be externally connected to the device, to provide corresponding functions. An input device may include a keyboard, a mouse, a touchscreen, a microphone, and various sensors. An output device may include a display, a speaker, a vibrator, and an indicator.

[0135] The communication interface 1140 is configured to connect to a communication module (not shown in the figure), to implement communication interaction between the device and another device. The communication module may implement communication in a wired manner (such as a USB and a network cable), or may implement communication in a wireless manner (such as a mobile network, WiFi, and Bluetooth).

[0136] The bus 1150 includes a path, for transmitting information between the components (for example, the processor 1110, the memory 1120, the input/output interface 1130, and the communication interface 1140) of the device.

[0137] It should be noted that although the foregoing device shows only the processor 1110, the memory 1120, the input/output interface 1130, the communication interface 1140, and the bus 1150, in a detailed implementation process, the device may further include other components required by normal running. In addition, a person skilled in the art may understand that the device may alternatively include only components necessary for implementing the solution of this embodiment of this specification and not necessarily include all components shown in the figure.

[0138] An embodiment of this specification further provides a computer-readable storage medium storing a computer program. The program, when executed by a processor, implements functions of the method shown in FIG. 1.

[0139] The computer-readable medium includes a persistent medium and a non-persistent 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 module of a program, or other data. Examples of computer storage media include, but are not limited to, a phase change memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), other type of random access memory (RAM), a read-only memory (ROM), an

electrically erasable programmable read-only memory (EEPROM), a flash memory or other memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or other optical storage, a cassette magnetic tape, tape and disk storage or other magnetic storage device or any other non-transmission media that may be configured to store information that a computing device can access. Based on the definition in the present disclosure, the computer readable medium does not include transitory computer readable media (transitory media), such as a modulated data signal and a carrier.

[0140] It may be learned from description of the foregoing implementations that, a person skilled in the art may clearly understand that the embodiments of this specification may be implemented by using software in addition to a necessary universal hardware platform. Based on such an understanding, the technical solutions of the embodiments of this specification essentially or the part contributing to the existing technologies may be implemented in a form of a software product. The computer software product may be stored in a storage medium, such as a ROM/RAM, a hard disk, or an optical disc, and includes a plurality of instructions for instructing a computer device (which may be a personal computer, a server, or a network device) to perform the methods described in the embodiments or some parts of the embodiments of this specification.

[0141] The system, the method, 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, and the specific form of the computer may be a personal computer, a laptop computer, a cellular telephone, 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 thereof.

[0142] In this specification, the embodiments are described in a progressive manner. Reference may be made to each other for the same or a similar part of the embodiments. Each embodiment focuses on a difference from other embodiments. Especially, apparatus and device embodiments are basically similar to a method embodiment, and therefore are described briefly; for related parts, refer to partial descriptions in the method embodiment. The method embodiment described above is merely an example. The modules described as separate parts may or may not be physically separate. During implementation of the solutions of the embodiments of this specification, the function of the modules may be implemented in the same piece of or a plurality of pieces of software and/or hardware. A part or all of the modules may be selected according to actual needs to achieve the objectives of the solutions

of the embodiments. A person of ordinary skill in the art may understand and implement this specification without creative efforts.

[0143] The foregoing descriptions are merely detailed implementations of the embodiments of this specification. It should be noted that a person of ordinary skill in the art may make several improvements and modifications without departing from the principle of the embodiments of this specification and the improvements and modifications shall fall within the protection scope of the embodiments of this specification.

CLAIMS

What is claimed is:

1. A transaction method based on centralized settlement and blockchain attestation, wherein a blockchain network comprises a plurality of member nodes, and the method comprises:

receiving, by a designated member node of the plurality of member nodes, a transaction request comprising a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount;

prior to a start of a consensus mechanism, performing, by the designated member node, transaction feasibility verification on the transaction request off the blockchain network, and performing, by the designated member node, an account balance modification operation off the blockchain network in a database after the verification is successful, the account balance modification operation comprising deducting the designated resource amount from a virtual resource account corresponding to the paying user identifier and adding the designated resource amount to a virtual resource account corresponding to the receiving user identifier, wherein the transaction feasibility verification comprises verifying whether a balance of the virtual resource account of the paying user is sufficient to provide the designated resource amount and whether the paying user has authorization; and

generating, by the designated member node, a log file recording the account balance modification operation performed off the blockchain network in the database, and broadcasting the log file to the blockchain network, for the member nodes to publish the log file to a blockchain based on the consensus mechanism.

2. The method according to claim 1, wherein the broadcasting the log file to the blockchain network comprises:

generating a log file summary corresponding to the log file according to the log file by using a hash algorithm; and

broadcasting the log file and the log file summary to the blockchain network, for the member nodes to publish the log file and the log file summary to the blockchain based on the consensus mechanism; and

the method further comprises:

sending the log file summary to the paying user and/or the receiving user, for the paying user and/or the receiving user to query the blockchain for the log file by using the log file summary.

3. The method according to claim 2, wherein the sending the log file summary to the paying user and/or the receiving user comprises:

sending the log file summary to the paying user and/or the receiving user if it is determined that the log file is published to the blockchain.

4. A transaction apparatus based on centralized settlement and blockchain attestation, wherein a blockchain network comprises a plurality of member nodes, the apparatus is a designated member node of the plurality of member node, and the apparatus comprises:

a receiving module, configured to receive a transaction request comprising a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount;

a settlement module, configured to: prior to a start of a consensus mechanism, perform transaction feasibility verification on the transaction request off the blockchain network, and perform an account balance modification operation off the blockchain network in a database after the verification is successful, the account balance modification operation being deducting the designated resource amount from a virtual resource account corresponding to the paying user identifier and adding the designated resource amount to a virtual resource account corresponding to the receiving user identifier, wherein the transaction feasibility verification comprises verifying whether a balance of the virtual resource account of the paying user is sufficient to provide the designated resource amount and whether the paying user has authorization; and

an attestation module, configured to generate a log file recording the account balance modification operation performed off the blockchain network in the database, and broadcast the log file to the blockchain network, for the member nodes to publish the log file to a blockchain based on the consensus mechanism.

5. The apparatus according to claim 4, wherein the attestation module generates a log file summary corresponding to the log file according to the log file by using a hash algorithm; and broadcasts the log file and the log file summary to the blockchain network, for the

member nodes to publish the log file and the log file summary to the blockchain based on the consensus mechanism; and

the apparatus further comprises:

a sending module, configured to send the log file summary to the paying user and/or the receiving user, for the paying user and/or the receiving user to query the blockchain for the log file by using the log file summary.

6. The apparatus according to claim 5, wherein the sending module sends the log file summary to the paying user and/or the receiving user if it is determined that the log file is published to the blockchain.

7. A transaction system based on centralized settlement and blockchain attestation, comprising a blockchain network formed by a plurality of member nodes, wherein

a designated member node of the plurality of member nodes receives a transaction request comprising a paying user identifier of a paying user, a designated resource amount, and a receiving user identifier of a receiving user, the paying user being a user paying the designated resource amount, and the receiving user being a user receiving the designated resource amount; prior to a start of a consensus mechanism, performs transaction feasibility verification on the transaction request, and performs an account balance modification operation off the blockchain network in a database after the verification is successful, the account balance modification operation being deducting the designated resource amount from a virtual resource account corresponding to the paying user identifier and adding the designated resource amount to a virtual resource account corresponding to the receiving user identifier, wherein the transaction feasibility verification comprises verifying whether a balance of the virtual resource account of the paying user is sufficient to provide the designated resource amount and whether the paying user has authorization; and generates a log file recording the account balance modification operation performed off the blockchain network in a database, and broadcasts the log file to the blockchain network; and

other member nodes and the designated member node publish the log file to a blockchain based on the consensus mechanism.

8. The system according to claim 7, wherein the designated member node generates a log file summary corresponding to the log file according to the log file by using a hash algorithm; and broadcasts the log file and the log file summary to the blockchain network, for

the member nodes to publish the log file and the log file summary to the blockchain based on the consensus mechanism; and sends the log file summary to the paying user and/or the receiving user, for the paying user and/or the receiving user to query the blockchain for the log file by using the log file summary.

9. The system according to claim 8, wherein the designated member node sends the log file summary to the paying user and/or the receiving user if it is determined that the log file is published to the blockchain.

10. A computer device, wherein a blockchain network comprises a plurality of member nodes, the device is a designated member node of the plurality of member nodes, wherein the device comprises a memory, a processor, and a computer program stored on the memory and executable on the processor, when executing the program, the processor implementing the method according to any of claims 1 to 3.