BUSINESS PROCESSING METHOD AND APPARATUS

Claim of Priority

This application claims priority to Chinese Patent Application No. 201710133969.X filed on March 8, 2017, the entire contents of which are hereby incorporated by reference.

Technical field

The present application relates to the field of computer technologies, and in particular, to a business processing method and apparatus.

Background art

At present, users may entrust some business handling organizations to handle some businesses for them, and these business handling organizations can provide professional business handling services for the users. The business handling organizations complete relatively complex and tedious business processing procedures for the users, while the users only need to pay certain fees. Therefore, business handling is made easy for the users.

For example, when needing to process a business through a business handling organization, a user may send a business request to the business handling organization by using a terminal held thereby. The business handling organization may obtain a corresponding business result according to the business request sent by the user, and return the business result to the user.

However, in actual applications, some business handling organizations may have some falsification behaviors in the process of handling businesses for users, and return incorrect business results to the users, thereby damaging benefits of the users.

By taking assets appraisal as an example, when handling an assets appraisal business through an assets appraisal organization (that is, a business handling organization), a user may send assets data to be appraised and a valid personal certificate to the assets appraisal organization in a manner of a business request. After receiving the business request, the assets appraisal organization may provide a false assets appraisal report intentionally, and return the assets appraisal report to the user as a business result. In this case, the user may not be able to subsequently carry out transfer of a property right, insurance loss compensation, assets settlement, and other behaviors according to the assets appraisal report, thereby causing a loss to the property of the user to some extent.

It can be seen from the above illustration that the process of carrying out business handling by a user through a business handling organization lacks trust guarantee, and therefore, certain loss may be caused during business processing. How to construct a reliable trust mechanism between a user and a business handling organization to protect the user from losses during business processing is an urgent problem to be solved.

Summary of the Invention

Embodiments of the present application provide a business processing method, to solve the problem in the prior art that a user may suffer losses when processing a business through a business handling organization.

The embodiments of the present application provide a business processing method, including:

receiving, by a first block chain node, business information sent by a user;

generating a corresponding business request according to the business information, the business request including a first smart contract generated according to the business information; and

sending the business request to a consensus network, such that a third block chain node in the consensus network obtains a corresponding business result according to the business request, and executing a first designated operation by triggering the first smart contract when it is determined that a second block chain node in the consensus network verifies the business result as legal.

The embodiments of the present application provide a business processing apparatus, to solve the problem in the prior art that a user may suffer losses when processing a business through a business handling organization.

The embodiments of the present application provide a business processing apparatus, including:

a receiving module configured to receive business information sent by a user;

a generation module configured to generate a corresponding business request according to the business information, the business request including a first smart contract generated according to the business information; and

a sending module configured to send the business request to a consensus network, such that a third block chain node in the consensus network obtains a corresponding business result according to the business request, and execute a first designated operation by triggering the first smart contract when it is determined that a second block chain node in the consensus network verifies the business result as legal.

Embodiments of the present application provide a business processing method, to solve the problem in the prior art that a user may suffer losses when processing a business through a business handling organization.

The embodiments of the present application provide a business processing method, including:

acquiring, by a second block chain node from a consensus network, business feedback information sent by a third block chain node;

acquiring a business result from the third block chain node according to the business

feedback information, the business result being generated by the third block chain node according to a business request sent by a first block chain node to the consensus network; and

when the business result is verified as legal, enabling the first block chain node to execute a first designated operation by triggering a first smart contract.

The embodiments of the present application provide a business processing apparatus, to solve the problem in the prior art that a user may suffer losses when processing a business through a business handling organization.

The embodiments of the present application provide a business processing apparatus, including:

an information acquisition module configured to acquire, from a consensus network, business feedback information sent by a third block chain node;

a result acquisition module configured to acquire a business result from the third block chain node according to the business feedback information, the business result being generated by the third block chain node according to a business request sent by a first block chain node to the consensus network; and

a verification module configured to, when verifying the business result as legal, enable the first block chain node to execute a first designated operation by triggering a first smart contract.

Embodiments of the present application provide a business processing method, to solve the problem in the prior art that a user may suffer losses when processing a business through a business handling organization.

The embodiments of the present application provide a business processing method, including:

acquiring, by a third block chain node, a business request sent by a first block chain node by using a consensus network, the business request including a first smart contract generated by the first block chain node according to business information sent by a user;

obtaining a business result and business feedback information according to the business request; and

sending the business feedback information to the consensus network, such that a second block chain node in the consensus network acquires the business result from the third block chain node according to the business feedback information, and when the business result is verified as legal, enabling the first block chain node to execute a first designated operation by triggering the first smart contract.

The embodiments of the present application provide a business processing apparatus, to solve the problem in the prior art that a user may suffer losses when processing a business through a business handling organization.

The embodiments of the present application provide a business processing apparatus, including:

a request acquisition module configured to acquire a business request sent by a first block chain node by using a consensus network, the business request including a first smart contract generated by the first block chain node according to business information sent by a user;

an information generation module configured to obtain a business result and business feedback information according to the business request; and

an information sending module configured to send the business feedback information to the consensus network, such that a second block chain node in the consensus network acquires the business result from the apparatus according to the business feedback information, and when the business result is verified as legal, enable the first block chain node to execute a first designated operation by triggering the first smart contract.

The at least one above technical solution used in the embodiments of the present application can achieve the following beneficial effects:

In the embodiments of the present application, a first block chain node utilizes a smart contract that can be executed automatically. Therefore, the first block chain node can execute a first designated operation by triggering the first smart contract once a business result obtained by a third block chain node according to a business request sent by the first block chain node passes verification carried out by a second block chain node. The designated operation during business processing can be completed fairly without manual intervention. Moreover, because the second block chain node can verify the business result obtained by the third block chain node, the whole business processing procedure is provided with a system of impartiality, thus greatly improving the impartiality of business processing, and reducing the possibility that a user suffers losses during business processing.

Brief Description of the Drawings

The accompanying drawings described herein are used to provide further understanding of the present application, and construct a part of the present application. Exemplary embodiments of the present application and illustrations thereof are used to explain the present application, but are not intended to form any improper limitation on the present application. In the accompanying drawings:

FIG. 1 is a schematic diagram of a user carrying out business processing by using a consensus network of block chains according to an embodiment of the present application;

FIG. 2 is a schematic diagram of a business processing procedure according to an embodiment of the present application;

FIG. 3 is a schematic diagram of a business processing apparatus according to an embodiment of the present invention;

FIG. 4 is a schematic diagram of a second business processing apparatus according to an embodiment of the present application; and

FIG. 5 is a schematic diagram of a third business processing apparatus according to an

embodiment of the present invention.

Detailed Description

In order to guarantee effective impartiality of a process in which a user carries out business processing through a business handling organization, in the present application, a trust mechanism may be established between the user and the business handling organization by using a consensus network of block chains. That is, by means of the tamper-resistant characteristic of data stored in the block chains of the consensus network, a business request sent by the user and a business result obtained by the business handling organization according to the business request both have effective impartiality. Moreover, to further improve impartiality during business processing, an audit department is further introduced as a block chain node in the present application to verify the business request sent by the user and the business result obtained by the business handling organization. After the verification succeeds, a smart contract is triggered by means of signing to automatically execute a designated operation, thereby implementing a process of automatically completing business processing without manual intervention. Relationships among the user, the business handling organization, and the audit department are as shown in FIG. 1.

FIG. 1 is a schematic diagram of a user carrying out business processing by using a consensus network of block chains according to an embodiment of the present application.

In FIG. 1, the whole consensus network includes multiple block chain nodes. A terminal based on which the user sends a business request, the business handling organization, and the audit department are all block chain nodes in the whole consensus network. The user may send a business request to the consensus network by using the terminal that serves as a first block chain node. After the business request enters the consensus network, the business handling organization, as a third block chain node, can accept the business request and obtain a corresponding business result. Thereafter, the audit department, as a second block chain node, may verify the business result obtained by the third block chain node. After it is determined that the business result passes the verification, the audit department triggers, through signing, the first block chain node to execute a first designated operation by using the smart contract, that is, to transfer a certain amount of money in an account of the user to the business handling organization. Further, the business result obtained by the business handling organization and the business request sent by the user may further be stored in a block chain in the form of an information abstract, and this creates a basis for subsequent authentication on whether the business result and the business request have been modified.

In the embodiment of the present application, the business request sent by the user to the consensus network includes a first smart contract. With the first smart contract, the first block chain node can automatically execute the first designated operation by using the smart contract subsequently once the audit department, as the second block chain node, verifies the business

result obtained by the third block chain node according to the business request as legal.

Business result information generated by the third block chain node according to the business result includes a second smart contract. With the second smart contract, the third block chain node can execute a second designated operation by automatically triggering the smart contract subsequently once the second block chain node verifies the business result obtained by the third block chain node according to the business request as illegal. Here, "first" and "second" are merely used to distinguish different smart contracts from each other, and have no special meanings.

In order to make those skilled in the art better understand the technical solutions in the present application, the technical solutions in the embodiments of the present application will be described clearly and completely below in combination with the accompanying drawings in the embodiments of the present application. It is apparent that the described embodiments are merely some of embodiments of the present application, rather than all the embodiments. Based on the embodiments of the present application, all other embodiments derived by those of ordinary skill in the art without any creative effort shall fall within the protection scope of the present application.

FIG. 2 is a schematic diagram of a business processing procedure according to an embodiment of the present application, specifically including the following steps:

S201: A first block chain node receives business information sent by a user.

In an actual application, when the user needs to carry out business processing through a business handling organization, the user may send a business request to the business handling organization through a terminal, and the business request is generated by the terminal according to the business information input by the user in the terminal. For example, during assets appraisal, when intending to carry out real estate appraisal, the user may input in the terminal his/her valid certificate information, real estate information, and a reward demanded for this real estate appraisal. After receiving the information, the terminal may generate a corresponding real estate appraisal request according to the information.

On this basis, in the embodiment of the present application, the user may input corresponding business information in the terminal during business processing. In addition to inputting some information at a designated position of a terminal interface, the user may also upload some information to the terminal. The terminal mentioned here is the first block chain node in the consensus network.

It should be noted that, in the embodiment of the present application, in addition to being the terminal, the first block chain node may further be a designated client terminal in the terminal. The first block chain node may also be a server. That is, the user uploads business information to a server by using a terminal, and the server may generate a corresponding business request according to the received business information.

S202: A first smart contract matching the business information and a business request are generated according to the business information.

After receiving the business information sent by the user, the first block chain node may generate, according to the business information, a first smart contract matching the business information. In the embodiment of the present application, the function of the first smart contract lies in that: once a second block chain node verifies a business result generated by a third block chain node according to the business request sent by the first block chain node as legal, the first block chain node generally needs to execute a first designated operation by triggering the first smart contract. The first designated operation is, for example, transferring a part of designated resources in an account address of the user to an account address of the third block chain node. Therefore, the business information received by the first block chain node generally includes the account address of the user, as well as a reword (i.e., the designated resources) paid to the business handling organization (i.e., the third block chain node) for handling this business. Therefore, in the embodiment of the present application, the first block chain node may generate the first smart contract according to the account address of the user and the reward paid by the user to the business handling organization which are included in the business information. Definitely, the first smart contract may also be generated based on other business information.

In the embodiment of the present application, the first block chain node may compile the received business information by using a preset SOLC compiler to obtain the first smart contract. In addition, the first block chain node may also generate the first smart contract by using other compiling manners, which will not be exemplified one by one here.

After generating the first smart contract, the first block chain node may further generate a business request corresponding to the business information according to the received business information and the first smart contract. The business request may further include the account address of the user in addition to the first smart contract. Moreover, the business request may further include abstract information of the business information. The abstract information is included because the first block chain node needs to send the business request to the consensus network subsequently, and generally, all block chain nodes in the whole consensus network may view the business request in the consensus network, and if the business request directly includes the business information uploaded by the user in the first block chain node, user information may be leaked, thus causing inconvenience to the user.

For example, assuming that the user requires real estate appraisal, it is generally necessary for the user to send his/her detailed real estate information to the first block chain node (if the first block chain node is a service platform, the service platform needs to be a qualified platform certificated by a related department, that is, the service platform will not leak information uploaded by the user). If the first block chain node does not process the real estate information sent by the user but directly adds the real estate information to the generated business request,

once the business request enters the whole consensus network, the block chain nodes in the consensus network will inevitably view the real estate information of the user, thus causing leakage of the user information.

Therefore, to protect the business information sent by the user from being leaked, in the embodiment of the present application, the first block chain node will generate, according to the received business information, an information abstract of the business information (definitely, data desensitization process may also be performed on the business information), add the information abstract to the business request, and send the business request to the consensus network. In this way, although all the block chain nodes in the consensus network can view the business request, they can only view the information abstract in the business request and cannot obtain the real business information actually corresponding to the information abstract, thereby protecting the user information from being leaked.

In addition, another purpose of the information abstract is as follows: as the information abstract is generated by the first block chain node by using a preset information abstract algorithm and the received business information, the business information and the information abstract have a unique corresponding relationship. That is, once content of the business information is changed, an information abstract generated by using the preset information abstract algorithm is definitely different from the previous information abstract (that is, the information abstract generated before the content of the business information is changed). In this way, the objective of effectively checking whether the user or another person (or a block chain node) has actively modified the business information in the subsequent procedure can be achieved.

It should be noted that, in addition to being generated by the first block chain node according to the business information sent by the user, the first smart contract may further be compiled by the user. Correspondingly, the user may send the compiled first smart contract to the first block chain node, such that the first block chain node generates a business request including the first smart contract according to the business information sent by the user and the first smart contract.

S203: The business request including a first smart contract in a check pending state is sent to the consensus network.

After obtaining the business request, the first block chain node may send the business request to the consensus network. The first block chain node may send the business request to the consensus network in a form of transaction. For example, a small-amount transaction is initiated, and the business request is carried in the transaction and then sent to the consensus network, such that when the third block chain node accepts this transaction subsequently, the third block chain node also accepts the business request.

Generally speaking, the smart contract needs a certain triggering condition for executing various actions. The triggering condition here may be implemented by changing the state of the

smart contract. Therefore, in the embodiment of the present application, the first smart contract has different states in different stages. Once the state is changed, the first smart contract is triggered to transform to the next stage, that is, a different action is triggered to be executed. On this basis, when the first block chain node sends the business request to the consensus network, the state of the first smart contract in the business request may be changed from an initial non-state to a check pending state, such that the second block chain node verifies, in a subsequent procedure, the legality of the business request including the first smart contract in the check pending state.

Definitely, when the first block chain node generates the first smart contract according to the received business information, the first smart contract is in the check pending state. In other words, once the first smart contract is generated, an initial state thereof is the check pending state. Thereafter, the first block chain node may send the business request including the first smart contract in the check pending state to the consensus network, such that the second block chain node in the consensus network verifies the legality of the business request.

S204: The second block chain node acquires, from the first block chain node according to the business request, business information corresponding to the business request.

In the embodiment of the present application, the block chain nodes in the consensus network may have multiple business requests, and different business requests may be in different business processing stages. For example, some business requests may be just sent from the first block chain node to the consensus network, and some business requests may be executed to some extent. Marking the business processing stages of the business requests may be implemented by using states of smart contracts included in the business requests. Therefore, for some business requests that just enter the consensus network, the second block chain node (that is, the audit department) in the consensus network needs to check the business requests including first smart contracts in the check pending state, and further verify the legality of such business requests in the subsequent procedure.

S205: It is verified whether the business information is legal, and if yes, step S206 is performed; or if no, step S207 is performed.

S206: Signing is performed on the business request, such that the state of the first smart contract is changed from the check pending state to an acceptance pending state, and the first block chain node freezes a first set quantity of designated resources in an account address of the user in the business request by using the first smart contract in the acceptance pending state.

S207: No signature is made on the business request, such that the first block chain node determines that the business request is failed to be accepted.

When viewing the business request including the first smart contract in the check pending state from the consensus network, the second block chain node needs to verify the legality of the business request. The verification is conducted because in an actual application, the business

handling organization may cheat the user, and the user may also cheat the business handling organization. For example, when carrying out real estate appraisal through the business handling organization, the user may provide false real estate information inconsistent with reality to the business handling organization, such that the business handling organization obtains a real estate appraisal report (i.e., a business result) inconsistent with reality according to the real estate information provided by the user. By using the true real estate information, the user may then sue against the business handling organization for the real estate appraisal report inconsistent with reality. This may adversely affect the business handling organization.

Therefore, to avoid the above situation, in the embodiment of the present application, before the third second block chain node accepts and processes the business request sent by the first second block chain node, the second block chain node (i.e., the audit department) may first verify the business request to ensure the legality of the business request.

Specifically, when viewing the business request including the first smart contract in the check pending state in the consensus network, the second block chain node may acquire, from the first block chain node, business information sent by the user to the first block chain node, and verify the legality of the business information. If the business information is verified as legal, the second block chain node may sign on the business request in the consensus network. Once the business request is signed by the second block chain node, the first smart contract in the business request will be changed from the check pending state to the acceptance pending state. In this way, the third block chain node may subsequently accept the business request including the first smart contract in the acceptance pending state. In other words, as the second block chain node makes the signature on the business request, it is guaranteed to some extent that the business request accepted by the third block chain node is a legal business request.

At the same time, once the second block chain node signs on the business request, the block chain nodes in the whole consensus network may establish a consensus about the business request. Once the consensus is established, the business request will be recorded in block chains in the consensus network, that is, block chains of the block chain nodes. The information recorded in the block chains is tamper-resistant, and therefore, after being recorded in the block chains, the business request may be used in a subsequent procedure for verifying whether the business information sent by the user and the business result obtained by the third block chain node (that is, the business handling organization) according to the business information have been modified (as the business request includes the information abstract generated by the first block chain node according to the business information), thereby further guaranteeing impartiality of the whole business processing.

Moreover, once the second block chain node determines the business information as legal and signs on the business request, the first block chain node may freeze the first set quantity of designated resources in the account address of the user by using the first smart contract in the

acceptance pending state, for use in subsequent business settlement.

In addition to verifying whether the business information acquired from the first block chain node is legal, the second block chain node further needs to verify whether the business information uniquely corresponds to the information abstract in the business request, and whether the first smart contract in the business request is reasonably made. Definitely, the second block chain node also needs to analyze, by using a public key (or a private key) held by itself, the account address of the user included in the business request, and determine the legality of the account address. Once the second block chain node verifies all the above items as legal, signing is performed on the business request, such that the block chain nodes in the consensus network establish a consensus about the business request, and the state of the first smart contract in the business request is triggered to be changed from the check pending state to an acceptance pending state. Whether the second block chain node uses a public key or a private key to analyze the account address of the user included in the business request depends on whether the first block chain node uses a private key or a public key when generating the business request.

When the second block chain node verifies the business request as illegal (for example, the account address of the user is illegal, the business information is inconsistent with the information abstract in the business request, the first smart contract is made unreasonably, and the business information is illegal), no signature is made on the business request, such that the first block chain node determines that the business request is failed to be accepted, and returns a message indicating failure in acceptance of the business request to the user. The manner of determining, by the first block chain node, that the business request is failed to be accepted may be: when the first block chain node monitors, by using the first smart contract in the business request, that the second block chain node still does not sign on the business request after first set duration, the message indicating that the business request is failed to be accepted is automatically triggered by using the first smart contract to be returned to the first block chain node. Therefore, the user learns, according to the message received by the first block chain node, that the business request sent by using the first block chain node fails to pass the auditing carried out by the second block chain node. Definitely, in the embodiment of the present application, once verifying the business request as illegal, the second block chain node may directly send to the first block chain node the message indicating that the business request fails to pass the auditing.

It should be noted that, in the embodiment of the present application, the second block chain node is the audit department that can audit the business request and the business result sent by the business handling organization. Therefore, the second block chain node has a permission of acquiring the business information from the first block chain node. Considering that it is necessary to protect the business information of the user from being acquired by an illegal organization and leaked, in the embodiment of the present application, when the second block chain node views the business request and needs to verify the legality of the business request, a

security certificate held by itself (i.e., the second block chain node) may be sent to the first block chain node, and the first block chain node may verify the qualification of the second block chain node by using the security certificate. Once it is determined that the second block chain node has the right to verify the legality of the business information sent by the user, the second block chain node may be authorized to acquire, from the first block chain node, the business information sent by the user; otherwise, the permission is not granted to the second block chain node.

S208: The third block chain node acquires the business request including the first smart contract in the acceptance pending state.

After verifying, by using the business request, the business information corresponding to the business request as legal, the second block chain node may sign on the business request to trigger the first smart contract in the business request to change from the check pending state to the acceptance pending state. The business request including the first smart contract in the acceptance pending state is a business request verified by the second block chain node (i.e., the audit department), and therefore, the business request is legal. As a result, the third block chain node (i.e., the business handling organization) may subsequently accept the business request including the first smart contract in the acceptance pending state. As known from the above step S203, the first block chain node may add the business request to a transaction and send the transaction to the consensus network. Therefore, the third block chain node can accept the transaction sent by the first block chain node, being equivalent to accepting the business request.

After the third block chain node receives the business request, the first smart contract in the business request will change from the acceptance pending state to a state of being accepted. This is because there may be multiple third block chain nodes in the whole consensus network in an actual application, that is, there may exist multiple business handling organizations. Generally, after one business handling organization accepts the business request, another business handling organization should no longer accept the business request. If the business request is accepted repeatedly, multiple business results may finally occur, which not only causes trouble to the user but also causes business disputes to the business handling organizations.

To avoid the above situation, in the embodiment of the present application, once a third block chain node accepts the business request, the first smart contract in the business request will change from the acceptance pending state to the state of being accepted. In this way, another third block chain node (i.e., another business handling organization) will not accept the business request again when viewing that the first smart contract in the business request is in the state of being accepted, thereby preventing the business request from being accepted repeatedly.

It should be noted that, in the embodiment of the present application, when the first block chain node sends the business request to the consensus network, generally, the block chain nodes (including the second block chain node and the third block chain node) in the consensus network

all receive the business request. In the embodiment of the present application, the state of the first smart contract needs to be synchronized among the block chain nodes. Therefore, when signing on the business request, the second block chain node may send a message indicating that the business request passes the verification to another block chain node in the consensus network. After the third block chain node in the consensus network receives the message, the first smart contract in the business request existing in the third block chain node may be automatically triggered to change its own state to the acceptance pending state. In this way, in the subsequent procedure, the third block chain node may process the business request including the first smart contract in the acceptance pending state.

In addition, in the embodiment of the present application, the first block chain node may first send the business request to the second block chain node in the consensus network. When it is determined that the business request passes the verification, the second block chain node may sign on the business request, such that the state of the first smart contract in the business request changes to the acceptance pending state. The business request including the first smart contract in the acceptance pending state is then further sent to the block chain nodes in the consensus network. At the same time, the second block chain node may return to the first block chain node a message indicating that the business request passes the verification, such that the first block chain node changes the state of the first smart contract of the business request stored therein to the acceptance pending state. Likewise, when receiving the business request including the first smart contract in the acceptance pending state, the third block chain node may receive and process the business request.

Definitely, in the embodiment of the present application, the second block chain node may also synchronize the state of the first smart contract by hedging. That is, the first block chain node may first send the business request to the block chain nodes in the consensus network. At this time, in the block chain nodes (including the second block chain node and the third block chain node), the states of the first smart contracts in the business requests are both the check pending state. When receiving the business request including the first smart contract in the check pending state, the third block chain node will not process the business request. At the same time, when receiving the business request including the first smart contract in the check pending state, other block chain nodes will not establish a consensus about the business request.

After receiving the business request, the second block chain node will verify the business request. Once the business request is verified as legal, the state of the first smart contract in the second block chain node may be changed by means of signing, that is, changed to the acceptance pending state. The second block chain node may then send the business request including the first smart contract in the acceptance pending state to the block chain nodes in the consensus network. After receiving the business request including the first smart contract in the acceptance pending state, the block chain nodes may cover (or remove) the previously-received business

request including the first smart contract in the check pending state, and establish a consensus about the business request including the first smart contract in the check pending state. At the same time, the third block chain node may process the business request to obtain a corresponding business result.

S209: A business result corresponding to the business request is obtained according to the business request.

After acquiring the business request, the third block chain node (i.e., the business handling organization) needs to obtain the corresponding business result according to the business request. The business request includes an abstract of information rather than the information itself, the third block chain node cannot obtain a reasonable business result according to the information abstract. Therefore, the third block chain node needs to acquire the business information corresponding to the information abstract from the first block chain node, thereby obtaining the corresponding business result according to the business information.

On this basis, in the embodiment of the present application, after acquiring the business request, the third block chain node may send a message for accepting the business request to the first block chain node. When the user views the message by using the first block chain node and allows the third block chain node to accept the business request sent by the user, a message for allowing the acceptance may be returned to the third block chain node by using the first block chain node, and the first block chain node is enabled to grant an access permission to the third block chain node. After receiving the message for allowing the acceptance returned by the first block chain node (i.e., after it is monitored that the first block chain node allows the third block chain node to accept the business request), the third block chain node acquires, from the first block chain node, the business information corresponding to the business request according to the access permission acquired from the block chain node and the business request. The first block chain node sets an access permission for the first block chain node so as to prevent some illegal organizations from acquiring and leaking the business information of the user, thereby avoiding causing losses to the user.

After acquiring the business information from the first block chain node, the third block chain node may obtain the business result corresponding to the business information according to the business information. The business result may be produced by a business handling specialist. The business handling specialist may upload the business result on the third block chain node, so that the business result is obtained.

S210: Business feedback information matching the business result is generated according to the business result, the business feedback information including a second smart contract obtained by the third block chain node according to the business request.

After the third block chain node obtains the business result, the business result needs to be audited by the second block chain node in the consensus network in the subsequent procedure.

The third block chain node cannot directly send the business information to the consensus network as the business result obtained by the third block chain node can reflect the business information of the user. If an illegal organization obtains the business result, an illegal operation may be carried out on property of the user according to the business result, thus causing losses to the user.

Therefore, in the embodiment of the present application, after the third block chain node acquires the business result from the first block chain node, it is necessary to generate the business feedback information matching the business result according to the obtained business result. The third block chain node may generate a result abstract of the business result by using a preset information abstract algorithm, add the result abstract to the subsequently generated business feedback information, and send the business feedback information to the consensus network. In addition to effectively preventing the business information from being leaked, the result abstract can further provide a powerful basis for subsequent verification on whether the third block chain node modifies the obtained business result (because the result abstract is uniquely corresponding to the business result, if content in the business result is changed, it is impossible to obtain a result abstract identical to the previous one according to the changed business result by using the same information abstract algorithm).

In addition, in the embodiment of the present application, the third block chain node may further generate a second smart contract matching the business result according to the obtained business result, and add the second smart contract to the subsequently generated business feedback information. This is because that, in an actual application, the business handling organization may cheat the user, that is, obtain a false business result according to real business information provided by the user, thus causing losses to the user. The business handling organization may refuse to admit the cheating behavior on the user, and therefore, the user may fail to obtain the corresponding compensation.

On this basis, in the embodiment of the present application, when the second block chain node (i.e., the audit department) verifies to-be-verified business result information sent by the third block chain node, if it is found that the business feedback information does not include the second smart contract capable of automatically triggering compensation for the user once there is a cheating behavior on the user (even if the third block chain node executes a second designated operation by using the second smart contract), the second block chain node does not accept the business feedback information, or determines that the business feedback information fails to be accepted. Therefore, in order that the business feedback information subsequently sent to the second block chain node can pass the verification carried out by the second block chain node, it is necessary for the third block chain node to generate a second smart contract matching the business request according to the business request, add the second smart contract to the subsequently generated business feedback information, and send the business feedback

information to the consensus network.

In the embodiment of the present application, when receiving, from the first block chain node, the business information corresponding to the business request, the third block chain node compiles the business information by using a preset SOLC compiler to obtain the second smart contract. Definitely, the third block chain node may also compile the second smart contract in other compiling manners, which will not be exemplified one by one here.

Definitely, in the embodiment of the present application, the business request includes the first smart contract, a reward paid by the user for this business handling is specified in the first smart contract, and the business request records a business type of the business. Therefore, the third block chain node may directly compile the business request by using the preset SOLC compiler to obtain the second smart contract matching the business request.

In addition, the third block chain node may make various second smart contracts in advance, different second smart contracts corresponding to different business types and business levels. For example, for a business request having a high business level, a second smart contract corresponding to such a type of business request may have a higher claim amount. Business requests of a same business level but different business types will correspond to different second smart contracts. Therefore, the third block chain node may specifically make different second smart contracts according to different business types and different business levels, and the made second smart contracts are stored in the third block chain node.

On this basis, in the embodiment of the present application, after gaining the business request including the first smart contract in the acceptance pending state, the third block chain node may further determine a business level and a business type of the business request, so as to determine a matching second smart contract according to the determined business level and business type as well as the first set quantity of designated resources specified in the first smart contract (e.g., the business reward specified by the user), then add the determined second smart contract to the generated business feedback information, and send the business feedback information to the consensus network.

It should be noted that, in the subsequent procedure, an account address of the third block chain node is required when the user pays the reward for the business handling to the third block chain node (i.e., the business handling organization) and when the third block chain node compensates the user. Therefore, in the embodiment of the present application, in addition to including the second smart contract and the result abstract as described above, the business feedback information generated by the third block chain node further includes the account address of the third block chain node. Furthermore, in the embodiment of the present application, once the second block chain node determines the business result obtained by the third block chain node as legal, it is necessary to sign on the business feedback information sent by the third block chain node, such that the second smart contract in the business feedback information is

triggered to trigger the first smart contract in the business request to execute an action of transferring the first set quantity of designated resources (e.g., a certain amount of money) in the user account to the account address of the third block chain node as the reward. Therefore, the second smart contract needs to be associated with the first smart contract in the business request, such that the second smart contract can trigger the first smart contract to execute the above action subsequently.

S211: The business feedback information is sent to the consensus network.

After obtaining the business feedback information, the third block chain node may send the business feedback information to the consensus network. When the business feedback information is sent to the consensus network, the second smart contract in the business feedback information will be changed from an initial non-state to a verification pending state. In this way, the second block chain node in the consensus network may acquire the business feedback information including the second smart contract in the verification pending state subsequently, and verify the legality of the business feedback information when it is determined that the second smart contract in the business feedback information is in the verification pending state.

Further, in the embodiment of the present application, once the third block chain node sends the business feedback information to the consensus network, the second smart contract in the business feedback information will trigger, by means of the state change, the third block chain node to freeze a second set quantity of designated resources (i.e., a certain amount of money for compensation) in the account address of the third block chain node by using the second smart contract. Therefore, it is guaranteed that in the subsequent procedure, once the business result obtained by the third block chain node according to the business request is verified as illegal, the third block chain node transfers this part of frozen designated resources to the account of the user by triggering the second smart contract.

It should be noted that, when sending the business feedback information, the third block chain node may add the business feedback information to a transaction, and send the transaction to the consensus network. The transaction may directly designate the second block chain node in the consensus network as a transaction object for transaction.

S212: The second block chain node acquires, from the consensus network, the business feedback information sent by the third block chain node.

After receiving the business feedback information that is sent by the third block chain node and includes the second smart contract in the verification pending state, the second block chain node may accept the business feedback information, that is, receive a transaction carrying the business feedback information, and further verify the legality of the business feedback information in the subsequent procedure.

S213: A business result corresponding to the business feedback information is acquired from the third block chain node according to the business feedback information.

After acquiring the business feedback information, the second block chain node needs to determine the business result corresponding to the business feedback information according to the business feedback information. The business feedback information does not include a real business result, but merely includes a result abstract uniquely corresponding to the business result (definitely, the business feedback information may also include the business result, but data desensitization needs to be carried out for the business result when the third block chain node sends the business result, so as to protect private information of the user). Therefore, the second block chain node needs to acquire the business result corresponding to the business feedback information from the third block chain node, and then verify the legality of the business result in the subsequent procedure.

The second block chain node (i.e., the audit department) is a department that can verify the legality of the business result obtained by the third block chain node. Therefore, generally, the second block chain node has the permission of directly acquiring the business result from the third block chain node. The third block chain node may also limit the permission of the second block chain node to more effectively protect the private information of the user from being leaked. Correspondingly, if the third block chain node limits the access permission of the second block chain node, when receiving and accepting the business feedback information sent by the third block chain node to the consensus network, the second block chain node may send a query message for accepting the business feedback information to the third block chain node, add a security certificate thereof to the query message, and send the query message to the third block chain node. After receiving the query message, the third block chain node may verify the security certificate.

Upon verification, if the security certificate has a qualification of verifying the business feedback information and the second block chain node is allowed to verify the business feedback information, a feedback message indicating acceptance approval may be returned to the second block chain node, and an access permission allowing acquisition of the business result from the third block chain node is granted to the second block chain node, such that the second block chain node acquires, from the third block chain node, the business result corresponding to the business feedback information on the basis of the access permission.

S214: It is verified whether the business result is legal, and if yes, step S215 is performed; or if no, step S216 is performed.

S215: Signing is performed on the business result information, such that the third block chain node triggers the second smart contract to enable the first block chain node to execute an action of transferring the first set quantity of designated resources in the account address of the user included in the business request to the account address of the third block chain node by using the first smart contract.

S216: No signature is made on the business result information, such that the third block

chain node transfers, by using the second smart contract, the second set quantity of designated resources in the account address of the third block chain node to the account address of the user.

When the second block chain node acquires, from the third block chain node, the business result corresponding to the business feedback information, the second block chain node may verify the legality of the business result. A specific verification manner may be: verifying the feasibility of the business result according to the business information as the second block chain node has acquired, from the first block chain node, the business information sent by the user to the first block chain node, so as to confirm whether the business result truly reflects actual conditions recorded by the business information and makes an effective and objective evaluation on the business information. If yes, the business result is determined as a legal business result; or if no, it is considered that the business result is cheating.

Further, in the embodiment of the present application, the second block chain node needs to parse the business feedback information by using a public key (or private key) held by itself to obtain the account address of the third block chain node included in the business feedback information, so as to determine whether the account address is legal and verify whether the second smart contract included in the business feedback information is applicable to the business information sent by the user at the first block chain node and the first smart contract included in the business request, for example, determine whether a compensation amount involved in the second smart contract matches the business type and business level of the business information and the business reward specified in the first smart contract. If the above aspects are all verified as legal, the business feedback information sent by the third block chain node is determined as legal; otherwise, the business feedback information is determined as illegal.

When the third block chain node verifies the business feedback information as legal, signing may be performed on the business feedback information to trigger the second smart contract in the business feedback information to change from the verification pending state to a verification successful state. Therefore, the third block chain node triggers, by using the second smart contract, the first smart contract associated with the second smart contract to transfer the first set quantity of designated resources (i.e., the reword paid to the business handling organization specified in the first smart contract) in the account address of the user in the business request to the account address of the third block chain node. At the same time, once the second block chain node signs on the business feedback information, the block chain nodes in the consensus network will establish a consensus about the business feedback information. After the consensus about the business feedback information is established, the business feedback information is written in the block chains in the consensus network. In other words, the block chain nodes may write the business feedback information, about which the consensus is established, into respective block chains. The data information written into the block chains is tamper-resistant. Therefore, it can be effectively verified, by using the result abstract included in the business

feedback information written into the block chains, whether the user or the business handling organization as the third block chain node modifies the corresponding business result subsequently, thereby providing a powerful basis for the verification on whether the business result is modified.

When the second block chain node verifies the business feedback information as illegal, no signature is made on the business feedback information. In this way, when it is monitored, by using the second smart contract, that the second block chain node still does not sign on the business feedback information after first set duration, the third block chain node may automatically trigger, by using the second smart contract, the action of transferring the second set quantity of designated resources (i.e., the money for compensation) in the account address of the third block chain node to the account of the user.

Further, once the second block chain node makes no signature on the business feedback information, the block chain nodes in the consensus network may not establish a consensus about the business feedback information, that is, the business feedback information is equivalently discarded.

It should be noted that the states of the second smart contract illustrated above in the block chain nodes in the consensus network need to be synchronized. The specific synchronization manner is similar to the state synchronization manner of the first smart contract, which is not described in detail. Once the second block chain node determines the business result obtained by the third block chain node according to the business information as legal and signs on the business feedback information, the state of the second smart contract of the business feedback information in the third block chain node will be changed, that is, changed to the verification successful state. In this case, the block chain node may send a message indicating that the business result is verified as legal to the first block chain node by using the second smart contract in the verification successful state. After receiving the message, the first block chain node may transfer, by using the first smart contract, the first set quantity of designated resources in the user account address to the account address of the third block chain node. In other words, the message sent by the third block chain node to the first block chain node may be considered as a condition for triggering the first block chain node to transfer the designated resources by using the first smart contract.

Definitely, when it is determined that the business result passes the verification, the second block chain node may send a message indicating that the business result passes the verification to the first block chain node. When monitoring, by using the first smart contract, that the second block chain node sends the message thereto, the first smart contract may trigger transfer of the first set quantity of designated resources in the user account address to the account address of the third block chain node by using the first smart contract.

After it is determined that the business result passes the verification carried out by the second

block chain node, the third block chain node may notify the first block chain node of the message indicating that the business result passes the verification. Therefore, after receiving the message, the first block chain node may acquire the business result from the third block chain node. Definitely, the third block chain node may also actively push the business result that passes the verification carried out by the second block chain node to the first block chain node.

Further, in the embodiment of the present application, after it is determined that the business result passes the verification, the second block chain node may also send the message indicating that the business request passes the verification to the first block chain node, such that the first block chain node acquires the business result from the second block chain node after receiving the message. Definitely, the second block chain node may also actively push the business request that passes the verification to the first block chain node.

It can be seen from the above method that the first block chain node and the third block chain node automatically accomplish payment of a reword or compensation by using a smart contract, no manual intervention is required. Moreover, the whole business handling process is implemented under the supervision and verification of the second block chain node, thereby effectively guaranteeing the impartiality of the whole business handling process. Further, once the business request sent by the first block chain node to the consensus network and the business feedback information sent by the third block chain node to the consensus network are verified as legal by the second block chain node, the block chain nodes in the consensus network will further establish a consensus about the business request and the business feedback information. After the consensus is established, the business request and the business feedback information are written into the block chains in the consensus network, thus providing a powerful basis for verification on whether the business information sent by the user and the business result obtained by the third block chain node are modified.

It should be noted that, in the embodiment of the present application, the verification on the legality of the business request and the business feedback information may be implemented by one second block chain node or multiple second block chain nodes. These second block chain nodes may be construed as some departments or organizations having credibility. These second block chain nodes may form a regional consortium chain consensus network. Correspondingly, when viewing the business request sent by the first block chain node in the whole consensus network, the second block chain nodes in the regional consortium chain consensus network may acquire business information corresponding to the business request from the first block chain node respectively, and verify the legality of the business information. Each second block chain node may then broadcast an obtained verification result to other second block chain nodes, such that the block chain nodes establish a consensus about the verification result, and obtain an overall final verification result. Further, a second block chain node currently serving as a leader node determines, according to the final verification result, whether to sign on the business

request.

Likewise, after the third block chain node sends the business feedback information to the consensus network, the second block chain node serving as a leader node in the regional consortium chain consensus network may accept the business feedback information, and instructs the second block chain nodes to acquire, from the third block chain node, the business results corresponding to the business feedback information. After acquiring the business results, the second block chain nodes may verify the legality of the business results respectively to obtain respective verification results. The second block chain nodes may then broadcast respective verification results to each other, such that the second block chain nodes in the regional consortium chain consensus network establish a consensus about the verification results and obtain a final verification result. Further, the second block chain node currently serving as the leader node determines, according to the final verification result, whether to sign on the business result information.

In the embodiment of the present application, after viewing the business request sent by the first block chain node, the second block chain node may not verify the legality of the business request first. Instead, the second block chain node verifies the legality of the business information corresponding to the business request as well as the legality of the business request at the same time after the third block chain node obtains the corresponding business result according to the business request.

In the embodiment of the present application, the second block chain node may receive the business request including the first smart contract and the user account address from the first block chain node and may receive the business feedback information including the second smart contract and the account address of the third block chain node from the third block chain node. Therefore, when the second block chain node verifies the business result as legal, the first set quantity of designated resources in the user account address may be transferred to the account address of the third block chain node by using the first smart contract. Likewise, when the second block chain node verifies the business result as illegal, the second set quantity of designated resources in the account address of the third block chain node may be transferred to the account address of the user by using the second smart contract.

In the process of verifying the legality of the business request and the business feedback information, if the business information corresponding to the business request and the business result corresponding to the business feedback information are overly complex, the second block chain node may ask a lawyer or another audit department to intervene, to implement the legality verification described above. The intervening lawyer or another audit department needs to sign a corresponding statement of responsibility, and the second block chain node writes the statement of responsibility into the block chain of the consensus network by initiating a transaction, for use when liability disputes occur subsequently.

In the embodiment of the present application, the first designated operation executed by the first block chain node by using the first smart contract may be transferring the first set quantity of designated resources in the user account address in the business request to the account address of the third block chain node, and may further be another designated operation. For example, the first designated operation may be used for enabling the first block chain node to automatically acquire the business result from the third block chain node or the second block chain node. For another example, the first designated operation may be used for enabling the first block chain node to determine a resource transfer time limit of transferring the first set quantity of designated resources in the user account address to the account address of the third block chain node, and after the resource transfer time limit expires, the first block chain node may transfer the first set quantity of designated resources in the user account address to the account address of the third block chain node. Definitely, the first designated operation may also be in other forms, which will not be exemplified one by one here.

Likewise, the second designated operation described above is not merely limited to enabling the third block chain node to transfer the second set quantity of designated resources in the account of the third block chain node to the account address of the user. For example, the second designated operation may also be used for enabling the third block chain node to change the state of the first smart contract in the business request (i.e., the business request received and processed by the third block chain node) to the acceptance pending state and send the business request to the consensus network, such that another block chain node capable of processing the business request can receive and process the business request. Definitely, the second designated operation may also be in other forms, which will not be exemplified one by one here.

It should be further noted that the business processing procedure described above is performed in the case of assets appraisal. For example, the first block chain node may be a terminal held by the user, the business information received by the first block chain node may be assets appraisal information and valid personal certificate information of the user that are sent by the user. The business request generated by the first block chain node according to the information sent by the user may be an assets appraisal request. The second block chain node may be an audit department that can carry out audition and supervision on the assets appraisal. The third block chain node may be an assets appraisal organization that can handle the assets appraisal business for the user. The business result obtained by the third block chain node according to the business information acquired from the first block chain node may be an assets appraisal report. The business feedback information sent to the second block chain node may be assets appraisal report information.

The business processing method described above can be used for assets appraisal, and can further be used for processing other businesses. For example, in real life, an accounting firm generally deals with businesses of applying for enterprise operation administrative licenses on

behalf of some enterprises or individuals. Generally, an individual or enterprise may submit a valid certificate thereof and enterprise data to the accounting firm. The accounting firm will obtain related materials according to the data and submit the materials to a related department (e.g., the industrial and commercial bureau) for examination and approval. If it is determined that the materials are consistent with actual situations of the individual or enterprise, the related department may grant an enterprise operation license to the individual or enterprise. In this process, the individual or enterprise pays a reward to the entrusted accounting firm, such that the accounting firm accomplishes related application for the enterprise operation license on behalf of the individual or enterprise.

The business processing method provided in the embodiment of the present application is also applicable to the scenario in which an accounting firm applies for an enterprise operation license on behalf of an individual or enterprise. That is, the individual or enterprise, as a client, may send enterprise data and a valid certificate thereof to a first block chain node. The first block chain node may generate a corresponding first smart contract and a business request according to the received materials, and send the business request to a consensus network. After viewing the business request, a related department (e.g., the industrial and commercial bureau) as a second block chain node may acquire, from the first block chain node, related data corresponding to the business request, and verify the legality of the related data. Once the data is verified as legal, signing may be performed on the business request, such that an accounting firm as a third block chain node can accept the signed business request, acquire from the first block chain node the related data sent by the individual or enterprise, and obtain corresponding related materials according to the acquired related data.

The accounting firm as the third block chain node may generate a corresponding second smart and a declaration application according to the obtained related materials, and send the declaration application to the consensus network. In this way, after viewing the declaration application from the consensus network, the second block chain node may acquire the related materials from the third block chain node, and verify the related materials according to the related data acquired from the first block chain node.

When verifying the related materials as legal, the second block chain node may sign on the declaration application sent by the third block chain node, such that the third block chain node triggers, by using the second smart contract, the first block chain node to execute automatic transfer of a certain amount money in an account address of the individual or enterprise as a reward to an account address of the accounting firm as the third block chain node by using the first smart contract in the business request. At the same time, the related department as the second block chain node may grant an enterprise operation license to the individual or enterprise. When verifying the related materials as illegal, the second block chain node does not sign the declaration application. In this way, when monitoring, by using the second smart contract in the

declaration application, that the second block chain node does not sign the declaration application after set duration, the third block chain node automatically triggers, by using the second smart contract, transfer of a certain amount of money in the account address of the accounting firm as a compensation to the account address of the individual or enterprise.

The scenario in which the accounting firm applies for an enterprise operation license for an individual or enterprise is used above to further illustrate the application range of the embodiment of the present application. In addition, the business processing method provided in the present application is also applicable to a scenario similar to the above two scenarios, and specific involved scenarios are not exemplified one by one here.

The business processing method provided in the embodiment of the present application is described in the foregoing, and based on the same idea, the embodiments of the present application further provide three types of business processing apparatuses, as shown in FIG. 3, FIG. 4 and FIG. 5.

FIG. 3 is a schematic diagram of a business processing apparatus according to an embodiment of the present application, specifically including:

a receiving module 301 configured to receive business information sent by a user;

a generation module 302 configured to generate a corresponding business request according to the business information, the business request including a first smart contract generated according to the business information; and

a sending module 303 configured to send the business request to a consensus network, such that a third block chain node in the consensus network obtains a corresponding business result according to the business request, and execute a first designated operation by triggering the first smart contract after it is determined that a second block chain node in the consensus network verifies the business result as legal.

The generation module 302 is configured to compile the business information by using a preset SOLC compiler to obtain the first smart contract.

The generation module 302 is configured to generate, according to the business information, the business request including the first smart contract and an account address of the user, the first designated operation being used for transferring a first set quantity of designated resources in the account address of the user to an account address of the third block chain node.

The sending module 303 is configured to send the business request including a first smart contract in a check pending state to the consensus network.

The sending module 303 is configured to, when it is determined that the second block chain node verifies the business request as legal, freeze the first set quantity of designated resources in the account address of the user by using the first smart contract.

The sending module 303 is configured to receive a query message, sent by the third block chain node, for processing the business request; grant an access permission to the third block

chain node when it is determined that the business request is processed by the third block chain node, such that the third block chain node acquires the business information from the apparatus and obtains the business result according to the business information.

The sending module 303 is configured to send the business request to block chain nodes in the consensus network to establish a consensus.

The sending module 303 is configured to write the business request into a block chain of the apparatus when it is determined that the consensus about the business request is established by the block chain nodes in the consensus network.

The sending module 303 is configured to acquire the business result from the third block chain node or the second block chain node when it is determined that the second block chain node verifies the business result as legal.

It should be noted that, in an actual application, the apparatus embodiment may have various improvements as required or select a specific implementation structure of a functional module, thereby obtaining a better technical effect.

For example, the sending module 303 may include a writing module 304. After the sending module 303 determines that the consensus about the business request is established by the block chain nodes in the consensus network, the writing module 304 may write the business request to the block chain of the apparatus. For another example, the sending module 303 may include an acquisition module 305. After the sending module 303 determines that the second block chain node verifies the business result as legal, the acquisition module 305 acquires the business result from the third block chain node or the second block chain node.

FIG. 4 is a schematic diagram of a second business processing apparatus according to an embodiment of the present application, specifically including:

an information acquisition module 401 configured to acquire, from a consensus network, business feedback information sent by a third block chain node;

a result acquisition module 402 configured to acquire a business result from the third block chain node according to the business feedback information, the business result being generated by the third block chain node according to a business request sent by a first block chain node to the consensus network; and

a verification module 403 configured to, when verifying the business result as legal, enable the first block chain node to execute a first designated operation by triggering the first smart contract.

The verification module 403 is configured to sign on the business feedback information; the signature being used for enabling a second smart contract included in the business feedback information to change its own state from a verification pending state to a verification successful state, and the second smart contract being obtained by the third block chain node according to the business request. The second smart contract in the verification successful state is used for

enabling the second smart contract to trigger the first block chain node to execute the first designated operation by using the first smart contract.

The verification module 403 is configured to, when verifying the business result as legal, instruct block chain nodes in the consensus network to establish a consensus about the business feedback information, and when it is determined that the consensus about the business feedback information is established, write the business feedback information into a block chain of the apparatus.

The verification module 403 is configured to, when verifying the business result as illegal, refuse to sign on the business feedback information. The refusing to sign is used for enabling the third block chain node to execute a second designated operation by triggering the second smart contract.

The information acquisition module 401 is configured to acquire a business request sent by the first block chain node to the consensus network, the business request including a first smart contract in a check pending state; acquire, from the first block chain node according to the business request, business information corresponding to the business request; verify whether the business information is legal; and if yes, sign on the business request to trigger the first smart contract to change from the check pending state to an acceptance pending state, the first smart contract in the acceptance pending state being used for enabling the first block chain node to freeze the first set quantity of designated resources in the account address of the user by using the first smart contract; or if no, refuse to sign on the business request, such that the first block chain node determines that the business request is failed to be accepted.

The verification module 403 is configured to, when verifying the business information as legal, notify block chain nodes in the consensus network to establish a consensus about the business request, and write the business request to the block chain of the apparatus when it is determined that the consensus about the business request is established.

It should be noted that, in an actual application, the apparatus embodiment may have various improvements as required or select a specific implementation structure of a functional module, thereby obtaining a better technical effect.

For example, the information acquisition module 401 may include a request verification module 404. After the information acquisition module 401 acquires the business request from the first block chain node, business information corresponding to the business request may be acquired from the first block chain node. The information acquisition module 401 may then verify whether the business information is legal by using the request verification module 404.

FIG. 5 is a schematic diagram of a third business processing apparatus according to an embodiment of the present application, specifically including:

a request acquisition module 501 configured to acquire a business request sent by a first block chain node via a consensus network, the business request including a first smart contract

generated by the first block chain node according to business information sent by a user;

an information generation module 502 configured to obtain a business result and a business feedback information according to the business request; and

an information sending module 503 configured to send the business feedback information to the consensus network, such that a second block chain node in the consensus network acquires the business result from the apparatus according to the business feedback information, and when the business result is verified as legal, enable the first block chain node to execute a first designated operation by triggering the first smart contract.

The request acquisition module 501 is configured to gain the business request including the first smart contract in an acceptance pending state.

The first designated operation is used for enabling the first block chain node to transfer a first set quantity of designated resources in an account address of the user included in the business request to an account address of the apparatus.

The information generation module 502 is configured to obtain a second smart contract and the business result according to the business request.

The information generation module 502 is configured to generate, according to the business result, the business feedback information including the second smart contract, abstract information of the business result, and the account address of the apparatus.

The information generation module 502 is configured to determine a business level and a business type of the business request; and determine the second smart contract according to the business level, the business type, and the first smart contract.

The information generation module 502 is configured to send, according to the business request, a query message for processing the business request to the first block chain node; acquire an access permission from the first block chain node when a feedback message that is returned by the first block chain node and allows the apparatus to process the business request is received; acquire, from the first block chain node, business information corresponding to the business request according to the business request and the access permission; and obtain the business result and the business feedback information according to the business information.

The information generation module 502 is configured to compile the business information by using a preset SOLC compiler to obtain the second smart contract.

The information sending module 502 is configured to send the business feedback information to the consensus network, and freeze a second set quantity of designated resources in the account address of the apparatus by triggering the second smart contract.

The information generation module 502 is configured to send the business feedback information to block chain nodes in the consensus network to establish a consensus, and write the business feedback information into a block chain of the apparatus when it is determined that the consensus about the business feedback information is established by the block chain nodes

in the consensus network.

The information sending module 502 is configured to execute a second designated operation by triggering the second smart contract when it is determined that the second block chain node verifies the business feedback information as illegal.

The second designated operation is used for enabling the apparatus to transfer a second set quantity of designated resources in the account address of the apparatus to the account address of the user included in the business request.

It should be noted that, in an actual application, the apparatus embodiment may have various improvements as required or select a specific implementation structure of a functional module, thereby obtaining a better technical effect.

For example, the information sending module 502 may include a writing module 504. After the information sending module 502 determines that the consensus about the business feedback information is established by the block chain nodes in the consensus network, the writing module 504 may write the business feedback information to the block chain of the apparatus.

In the embodiment of the present application, a first block chain node may send a business request generated according to business information sent by a user to a consensus network, such that when a second block chain node in the consensus network verifies a business result obtained by a third block chain node in the consensus network according to the business request as legal, the first block chain node is enabled to execute a first designated operation by using a first smart contract in the business request. The first block chain node utilizes the smart contract that can be executed automatically, such that once the business result obtained by the third block chain node according to the business request sent by the first block chain node passes the verification carried out by the second block chain node, the first block chain node may execute the first designated operation by triggering the first smart contract, and the designated operation in the business processing procedure can be accomplished fairly without manual intervention. Moreover, the second block chain node can verify the business result obtained by the third block chain node, such that the whole business processing procedure is provided with a system of impartiality, thereby greatly improving the impartiality of business processing, and reducing the probability that the user suffers losses during business processing.

In the 1990s, an improvement on a technology may be obviously distinguished as an improvement on hardware (for example, an improvement on a circuit structure such as a diode, a transistor, and a switch) or an improvement on software (an improvement on a method procedure). However, with the development of technologies, improvements of many method procedures at present may be considered as direct improvements on hardware circuit structures. Almost all designers program the improved method procedures into hardware circuits to obtain corresponding hardware circuit structures. Therefore, it is improper to assume that the improvement of a method procedure cannot be implemented by using a hardware entity module.

For example, a Programmable Logic Device (PLD) (for example, a Field Programmable Gate Array (FPGA)) is such an integrated circuit whose logic functions are determined by devices programmed by a user. Designers program by themselves to "integrate" a digital system into a piece of PLD, without the need to ask a chip manufacturer to design and manufacture a dedicated integrated circuit chip. Moreover, at present, the programming is mostly implemented by using logic compiler software, instead of manually manufacturing an integrated circuit chip. The logic compiler software is similar to a software complier used for developing and writing a program, and original code before compiling also needs to be written by using a specific programming language, which is referred to as a Hardware Description Language (HDL). There are many types of HDLs, such as Advanced Boolean Expression Language (ABEL), Altera Hardware Description Language (AHDL), Confluence, Cornell University Programming Language (CUPL), HDCal, Java Hardware Description Language (JHDL), Lava, Lola, MyHDL, PALASM, and Ruby Hardware Description Language (RHDL), among which Very-High-Speed Integrated Circuit Hardware Description Language (VHDL) and Verilog are most commonly used now. Persons skilled in the art also should know that a hardware circuit for implementing the logic method procedure may be easily obtained by slightly logically programming the method procedure using the above several hardware description languages and programming it into an integrated circuit.

A controller may be implemented in any suitable manner. For example, the controller may be in the form of, for example, a microprocessor or a processor and a computer readable medium storing computer readable program code (for example, software or firmware) executable by the (micro)processor, a logic gate, a switch, an Application Specific Integrated Circuit (ASIC), a programmable logic controller, and an embedded micro-controller. Examples of the controller include, but are not limited to, the following micro-controllers: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20, and Silicone Labs C8051F320. A memory controller may also be implemented as a part of control logic of a memory. Persons skilled in the art also know that the controller may be implemented by using pure computer readable program code, and in addition, the method steps may be logically programmed to enable the controller to implement the same function in a form of a logic gate, a switch, an application specific integrated circuit, a programmable logic controller and an embedded microcontroller. Therefore, this type of controller may be considered as a hardware component, and apparatuses included therein for implementing various functions may also be considered as structures inside the hardware component. Or, the apparatuses used for implementing various functions may even be considered as both software modules for implementing the method and structures inside the hardware component.

The system, apparatus, module or unit illustrated in the above embodiments may be specifically implemented by using a computer chip or an entity, or a product having a certain

function. A typical implementation device is a computer. Specifically, the computer may be, for example, a personal computer, a laptop computer, a cellular phone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an email device, a game console, a tablet computer, a wearable device, or a combination of any of these devices.

For ease of description, when the apparatus is described, it is divided into various units in terms of functions for respective description. Definitely, when the present application is implemented, functions of the units may be implemented in the same or multiple pieces of software and/or hardware.

Persons skilled in the art should understand that the embodiments of the present invention may be provided as a method, a system, or a computer program product. Therefore, the present invention may be implemented as a completely hardware embodiment, a completely software embodiment, or an embodiment combining software and hardware. Moreover, the present invention may be a computer program product implemented on one or more computer usable storage media (including, but not limited to, a magnetic disk memory, a CD-ROM, an optical memory, and the like) including computer usable program code.

The present invention is described with reference to flowcharts and/or block diagrams according to the method, device (system) and computer program product according to the embodiments of the present invention. It should be understood that a computer program instruction may be used to implement each process and/or block in the flowcharts and/or block diagrams and combinations of processes and/or blocks in the flowcharts and/or block diagrams. The computer program instructions may be provided to a general-purpose computer, a special-purpose computer, an embedded processor or another programmable data processing device to generate a machine, such that the computer or a processor of another programmable data processing device executes an instruction to generate an apparatus configured to implement functions designated in one or more processes in a flowchart and/or one or more blocks in a block diagram.

The computer program instructions may also be stored in a computer readable storage that can guide a computer or another programmable data processing device to work in a specific manner, such that the instruction stored in the computer readable storage generates a manufacture including an instruction apparatus, and the instruction apparatus implements functions designated by one or more processes in a flowchart and/or one or more blocks in a block diagram.

The computer program instructions may also be loaded in a computer or another programmable data processing device, such that a series of operation steps are executed on the computer or another programmable device to generate a computer implemented processing, and therefore, the instruction executed in the computer or another programmable device provides steps for implementing functions designated in one or more processes in a flowchart and/or one

or more blocks in a block diagram.

In a typical configuration, a computing device includes one or more processors (CPU), an input/output interface, a network interface, and a memory.

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

The computer readable medium includes non-volatile and volatile media as well as movable and non-movable media, and can implement information storage by means of any method or technology. Information may be a computer readable instruction, a data structure, and a module of a program or other data. A storage medium of a computer includes, for example, but is not limited to, a phase change memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), other types of RAMs, a ROM, an electrically erasable programmable read-only memory (EEPROM), a flash memory or other memory technologies, a compact disk read-only memory (CD-ROM), a digital versatile disc (DVD) or other optical storages, a cassette tape, a magnetic tape/magnetic disk storage or other magnetic storage devices, or any other non-transmission medium, and can be used to store information accessed by the computing device. According to the definition of this text, the computer readable medium does not include transitory media, such as a modulated data signal and a carrier.

It should be further noted that the term "include", "comprise" or other variations thereof are intended to cover non-exclusive inclusion, so that a process, method, commodity or device including a series of elements not only includes the elements, but also includes other elements not clearly listed, or further includes inherent elements of the process, method, commodity or device. In a case without any more limitations, an element defined by "including a/an..." does not exclude that the process, method, commodity or device including the element further has other identical elements.

Those skilled in the art should understand that the embodiments of the present application may be provided as a method, a system, or a computer program product. Therefore, the present application may be implemented as a completely hardware embodiment, a completely software embodiment, or an embodiment combining software and hardware. Moreover, the present application may be in the form of a computer program product implemented on one or more computer usable storage media (including, but not limited to, a magnetic disk memory, a CD-ROM, an optical memory and the like) including computer usable program code.

The present application may be described in a common context of a computer executable instruction executed by a computer, for example, a program module. Generally, the program module includes a routine, a program, an object, an assembly, a data structure, and the like used for executing a specific task or implementing a specific abstract data type. The present application may also be implemented in distributed computing environments, and in the

distributed computer environments, a task is executed by using remote processing devices connected through a communications network. In the distributed computer environment, the program module may be located in local and remote computer storage media including a storage device.

The embodiments in the specification are described progressively, identical or similar parts of the embodiments may be obtained with reference to each other, and each embodiment emphasizes a part different from other embodiments. Especially, the system embodiment is basically similar to the method embodiment, so it is described simply, and for related parts, reference may be made to the description of the parts in the method embodiment.

The above description is merely embodiments of the present application, and are not intended to limit the present application. For persons skilled in the art, the present application may have various modifications and variations. Any modification, equivalent replacement, improvement or the like made without departing from the spirit and principle of the present application should all fall within the scope of claims of the present application.

Embodiments and the operations described in this specification can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware, including the structures disclosed in this specification or in combinations of one or more of them. The operations can be implemented as operations performed by a data processing apparatus on data stored on one or more computer-readable storage devices or received from other sources. A data processing apparatus, computer, or computing device may encompass apparatus, devices, and machines for processing data, including by way of example a programmable processor, a computer, a system on a chip, or multiple ones, or combinations, of the foregoing. The apparatus can include special purpose logic circuitry, for example, a central processing unit (CPU), a field programmable gate array (FPGA) or an application-specific integrated circuit (ASIC). The apparatus can also include code that creates an execution environment for the computer program in question, for example, code that constitutes processor firmware, a protocol stack, a database management system, an operating system (for example an operating system or a combination of operating systems), a cross-platform runtime environment, a virtual machine, or a combination of one or more of them. The apparatus and execution environment can realize various different computing model infrastructures, such as web services, distributed computing and grid computing infrastructures.

A computer program (also known, for example, as a program, software, software application, software module, software unit, script, or code) can be written in any form of programming language, including compiled or interpreted languages, declarative or procedural languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, object, or other unit suitable for use in a computing environment. A program can be stored in a portion of a file that holds other programs or data (for example, one or more scripts

stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (for example, files that store one or more modules, sub-programs, or portions of code). A computer program can be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

Processors for execution of a computer program include, by way of example, both general- and special-purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read-only memory or a random-access memory or both. The essential elements of a computer are a processor for performing actions in accordance with instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data. A computer can be embedded in another device, for example, a mobile device, a personal digital assistant (PDA), a game console, a Global Positioning System (GPS) receiver, or a portable storage device. Devices suitable for storing computer program instructions and data include non-volatile memory, media and memory devices, including, by way of example, semiconductor memory devices, magnetic disks, and magneto-optical disks. The processor and the memory can be supplemented by, or incorporated in, special-purpose logic circuitry.

Mobile devices can include handsets, user equipment (UE), mobile telephones (for example, smartphones), tablets, wearable devices (for example, smart watches and smart eyeglasses), implanted devices within the human body (for example, biosensors, cochlear implants), or other types of mobile devices. The mobile devices can communicate wirelessly (for example, using radio frequency (RF) signals) to various communication networks (described below). The mobile devices can include sensors for determining characteristics of the mobile device's current environment. The sensors can include cameras, microphones, proximity sensors, GPS sensors, motion sensors, accelerometers, ambient light sensors, moisture sensors, gyroscopes, compasses, barometers, fingerprint sensors, facial recognition systems, RF sensors (for example, Wi-Fi and cellular radios), thermal sensors, or other types of sensors. For example, the cameras can include a forward- or rear-facing camera with movable or fixed lenses, a flash, an image sensor, and an image processor. The camera can be a megapixel camera capable of capturing details for facial and/or iris recognition. The camera along with a data processor and authentication information stored in memory or accessed remotely can form a facial recognition system. The facial recognition system or one-or-more sensors, for example, microphones, motion sensors, accelerometers, GPS sensors, or RF sensors, can be used for user authentication.

To provide for interaction with a user, embodiments can be implemented on a computer having a display device and an input device, for example, a liquid crystal display (LCD) or organic light-emitting diode (OLED)/virtual-reality (VR)/augmented-reality (AR) display for

displaying information to the user and a touchscreen, keyboard, and a pointing device by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, for example, visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, or tactile input. In addition, a computer can interact with a user by sending documents to and receiving documents from a device that is used by the user; for example, by sending web pages to a web browser on a user's client device in response to requests received from the web browser.

Embodiments can be implemented using computing devices interconnected by any form or medium of wireline or wireless digital data communication (or combination thereof), for example, a communication network. Examples of interconnected devices are a client and a server generally remote from each other that typically interact through a communication network. A client, for example, a mobile device, can carry out transactions itself, with a server, or through a server, for example, performing buy, sell, pay, give, send, or loan transactions, or authorizing the same. Such transactions may be in real time such that an action and a response are temporally proximate; for example an individual perceives the action and the response occurring substantially simultaneously, the time difference for a response following the individual's action is less than 1 millisecond (ms) or less than 1 second (s), or the response is without intentional delay taking into account processing limitations of the system.

Examples of communication networks include a local area network (LAN), a radio access network (RAN), a metropolitan area network (MAN), and a wide area network (WAN). The communication network can include all or a portion of the Internet, another communication network, or a combination of communication networks. Information can be transmitted on the communication network according to various protocols and standards, including Long Term Evolution (LTE), 5G, IEEE 802, Internet Protocol (IP), or other protocols or combinations of protocols. The communication network can transmit voice, video, biometric, or authentication data, or other information between the connected computing devices.

Features described as separate implementations may be implemented, in combination, in a single implementation, while features described as a single implementation may be implemented in multiple implementations, separately, or in any suitable sub-combination. Operations described and claimed in a particular order should not be understood as requiring that the particular order, nor that all illustrated operations must be performed (some operations can be optional). As appropriate, multitasking or parallel-processing (or a combination of multitasking and parallel-processing) can be performed.

CLAIMS

1. A business processing method, comprising:

receiving, by a first block chain node, business information sent by a user;

generating a corresponding business request according to the business information, the business request comprising a first smart contract generated according to the business information;

sending the business request to a consensus network, such that a third block chain node in the consensus network obtains a corresponding business result according to the business request, and

executing a first designated operation by triggering the first smart contract when it is determined that a second block chain node in the consensus network verifies the business result as legal comprising:

acquiring, by the second block chain node from the consensus network, business feedback information sent by the third block chain node;

acquiring the business result from the third block chain node according to the business feedback information, the business result being generated by the third block chain node according to the business request sent by the first block chain node to the consensus network; and

when the business result is verified as legal, enabling the first block chain node to execute the first designated operation by triggering the first smart contract, wherein the step of enabling the first block chain node to execute the first designated operation by triggering the first smart contract specifically comprises:

signing on the business feedback information to generate a signature;

the signature being used for enabling a second smart contract comprised in the business feedback information to change its own state from a verification pending state to a verification successful state, the second smart contract being obtained by the third block chain node according to the business request; and

the second smart contract in the verification successful state being used for enabling the second smart contract to trigger the first block chain node to execute the first designated operation by using the first smart contract.

2. The method of claim 1, wherein the step of generating the first smart contract according to

the business information specifically comprises:

compiling the business information by using a preset SOLC compiler to obtain the first smart contract.

3. The method of claim 1 or 2, wherein the step of generating the corresponding business request according to the business information specifically comprises:

generating a business request comprising the first smart contract and an account address of the user according to the business information;

the first designated operation being used for transferring a first set quantity of designated resources in the account address of the user to an account address of the third block chain node, optionally wherein after the step of sending the business request to the consensus network, the method further comprises:

freezing the first set quantity of designated resources in the account address of the user by using the first smart contract when it is determined that the second block chain node verifies the business request as legal.

4. The method of claim 1, wherein the step of sending the business request to the consensus network specifically comprises:

sending the business request comprising the first smart contract in a check pending state to the consensus network.

5. The method of claim 1, wherein after the step of sending the business request to the consensus network, the method further comprises:

receiving a query message, sent by the third block chain node, for processing the business request; and

granting an access permission to the third block chain node when it is determined that the business request is processed by the third block chain node, such that the third block chain node acquires the business information from the first block chain node, and obtains the business result according to the business information.

6. The method of claim 1, wherein the step of sending the business request to the consensus

network specifically comprises:

sending the business request to block chain nodes in the consensus network to establish a consensus; and

the method further comprises:

writing the business request into a block chain of the first block chain node after it is determined that the block chain nodes in the consensus network establish a consensus about the business request.

7. The method of claim 1, wherein the method further comprises:

acquiring the business result from the third block chain node or the second block chain node when it is determined that the second block chain node verifies the business result as legal.

8. The method of any one of the preceding claims, wherein the method further comprises:

instructing block chain nodes in the consensus network to establish a consensus about the business feedback information when the business result is verified as legal, and writing the business feedback information into a block chain of the second block chain node when it is determined that the consensus about the business feedback information is established.

9. The method of any one of the preceding claims, wherein the method further comprises:

refusing to sign on the business feedback information when the business result is verified as illegal; and

the refusing to sign being used for enabling the third block chain node to execute a second designated operation by triggering the second smart contract.

10. The method of any one of claims 8 to 9, wherein before the step of acquiring, by the second block chain node from the consensus network, business feedback information sent by the third block chain node, the method further comprises:

acquiring a business request sent by the first block chain node to the consensus network, the business request comprising the first smart contract in a check pending state;

acquiring, according to the business request, business information corresponding to the business request from the first block chain node;

verifying whether the business information is legal; and

if yes, signing on the business request to trigger the first smart contract to change from the check pending state to an acceptance pending state; the first smart contract in the acceptance pending state being used for enabling the first block chain node to freeze a first set quantity of designated resources in an account address of the user by using the first smart contract; or

if no, refusing to sign on the business request, such that the first block chain node determines that the business request is failed to be accepted,

wherein the method further comprises:

instructing the block chain nodes in the consensus network to establish a consensus about the business request when the business information is verified as legal, and writing the business request into a block chain of the second block chain node after it is determined that the consensus about the business request is established.

11. The method of any one of the preceding claims, further comprising:

acquiring, by the third block chain node, the business request sent by the first block chain node by using the consensus network, the business request comprising the first smart contract generated by the first block chain node according to business information sent by the user (S208);

obtaining the business result and business feedback information according to the business request (S209); and

sending the business feedback information to the consensus network (S211), such that the second block chain node in the consensus network acquires the business result from the third block chain node according to the business feedback information (S213), and when the business result is verified as legal, enabling the first block chain node to execute the first designated operation by triggering the first smart contract (S215).

12. The method of claim 11 wherein the step of acquiring, by the third block chain node, the business request sent by the first block chain node by using the consensus network specifically comprises:

gaining the business request comprising the first smart contract in an acceptance pending state.

13. The method of claim 11, wherein the first designated operation is used for enabling the first block chain node to transfer a first set quantity of designated resources in an account address of the user comprised in the business request to an account address of the third block chain node;

the step of obtaining a business result according to the business request specifically comprises:

obtaining a second smart contract and the business result according to the business request;

the step of obtaining business feedback information according to the business request specifically comprises:

generating, according to the business result, the business feedback information comprising the second smart contract, abstract information of the business result, and the account address of the third block chain node, wherein the step of obtaining the second smart contract according to the business request specifically comprises:

determining a business level and a business type of the business request; and

determining the second smart contract according to the business level, the business type, and the first smart contract.

14. The method of claim 11, wherein the step of obtaining a business result and business feedback information according to the business request specifically comprises:

sending, according to the business request, a query message for processing the business request to the first block chain node;

acquiring an access permission from the first block chain node when a feedback message is received, the feedback message being returned by the first block chain node and allowing the third block chain node to process the business request;

acquiring, from the first block chain node, business information corresponding to the business request according to the business request and the access permission; and

obtaining the business result and business feedback information according to the business information, wherein the step of obtaining a second smart contract according to the business request specifically comprises:

compiling the business information by using a preset SOLC compiler to obtain the second smart contract.

15. The method of claim 13, wherein the step of sending the business feedback information to the consensus network specifically comprises:

sending the business feedback information to the consensus network, and freezing a second set quantity of designated resources in the account address of the third block chain node by triggering the second smart contract.

16. The method of any one of claims 11 to 15, wherein the step of sending the business feedback information to the consensus network specifically comprises:

sending the business feedback information to block chain nodes in the consensus network to establish a consensus, and writing the business feedback information into a block chain of the third block chain node when it is determined that the consensus about the business feedback information is established by the block chain nodes in the consensus network.

17. The method according to claim 11 or 13, wherein the method further comprises:

executing a second designated operation by triggering the second smart contract when it is determined that the second block chain node verifies the business feedback information as illegal,

wherein the second designated operation is used for transferring, by the third block chain node, a second set quantity of designated resources in the account address of the third block chain node to the account address of the user comprised in the business request.

18. A business processing apparatus, comprising:

a plurality of modules, each module configured to perform steps in the method of any one of claims 1 to 17.