TRANSACTION PROCESSING METHOD AND APPARATUS

TECHNICAL FIELD

[0001] One or a plurality of embodiments of the present specification relate to the field of computers, and in particular, to a transaction processing method and apparatus.

BACKGROUND

[0002] Current transaction processing usually requires the participation of multiple parties. For example, a transaction may involve a transaction initiator and one or a plurality of transaction-related parties. With the development of the blockchain technology, the blockchain technology has been used in the process of transaction processing to store transaction data exchanged among multiple parties.

[0003] Once the transaction data is recorded on a blockchain network, repudiation or data tampering of individual blockchain members can be prevented, the basis of which is that everyone participates in recording and each blockchain member can get all data on the blockchain network. If the transaction data contains sensitive data (for example, user privacy data) and the sensitive data is written to the blockchain, the sensitive data will be leaked to all blockchain members.

[0004] As a result, there is a desire for an improved solution that does not cause leakage of sensitive data when transaction data is stored by using a blockchain network.

SUMMARY

[0005] One or a plurality of embodiments of the present specification describe a transaction processing method and apparatus, wherein sensitive data will not be leaked when transaction data is stored by using a blockchain network.

[0006] In a first aspect, a transaction processing method is provided, the method is performed by a transaction initiator, and the method comprising:

[0007] sending a transaction confirmation request for a target transaction to each transaction-related party, the transaction confirmation request comprising transaction data;

[0008] receiving a transaction confirmation response from each of the transaction-related parties, the transaction confirmation response comprising a first data block and first signed data, wherein the first data block comprises first encoded data generated by encoding the transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; and the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party;

[0009] encoding the transaction data using the preset encoding method to generate second encoded data; and generating a second confirmation result;

[0010] signing, by using a private key of the transaction initiator, a second data block comprising the second encoded data, the second confirmation result, and an identifier of the transaction initiator, so as to obtain second signed data; and

[0011] storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator through a blockchain network when determining that each of the first confirmation results and the second confirmation result are Confirmed.

[0012] In one possible implementation, the method further comprises:

[0013] processing the target transaction through the blockchain network when determining that each of the first confirmation result and the second confirmation result are Confirmed.

[0014] Further, processing the target transaction through the blockchain network comprises:

[0015] recording processing result information of the target transaction through the blockchain network; and

[0016] sending the processing result information of the target transaction to each of the transaction-related parties through the blockchain network, so that each of the transaction-related parties processes the target transaction.

[0017] In a second aspect, a transaction processing method performed by a transaction-related party is provided, comprising:

[0018] receiving a transaction confirmation request for a target transaction from a transaction initiator, the transaction confirmation request comprising transaction data;

[0019] generating a first confirmation result according to the transaction data;

[0020] encoding the transaction data using a preset encoding method to generate first encoded data;

[0021] signing, by using a private key of the transaction-related party, a first data block comprising the first confirmation result and the first encoded data, so as to obtain first signed data; and

[0022] sending a transaction confirmation response to the transaction initiator, the transaction confirmation response comprising the first data block and the first signed data, so that the transaction initiator stores the first data block and the first signed data of each of the transaction-related parties and data of the transaction initiator through a blockchain network when determining that a confirmation result of each of the transaction-related parties is Confirmed.

[0023] In one possible implementation, the method further comprises:

[0024] receiving processing result information of the target transaction from the blockchain network; and

[0025] processing the target transaction according to the processing result information.

[0026] In a third aspect, a transaction processing method performed by a blockchain network is provided, comprising:

[0027] receiving, from a transaction initiator of a target transaction, a first data block and first signed data of each transaction-related party and a second data block and second signed data of the transaction initiator, wherein the first data block comprises first encoded data generated by encoding transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party; the second data block comprises second encoded data generated by encoding the transaction data using the preset encoding method by the transaction initiator, a second confirmation result, and an identifier of the transaction initiator; and the second signed data is obtained by performing signature computation on the second data block by using a private key of the transaction initiator; and

[0028] storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator.

[0029] In one possible implementation, after storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator, the method further comprises:

[0030] processing the target transaction.

[0031] Further, processing the target transaction comprises:

[0032] recording processing result information of the target transaction; and

[0033] sending the processing result information of the target transaction to each of the transaction-related parties, so that each of the transaction-related parties processes the target transaction.

[0034] Further, before storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator, the method further comprises:

[0035] performing the following checks:

[0036] checking whether the identifier of the transaction-related party and/or the identifier of the transaction initiator matches a member identifier on a transaction link of the target transaction;

[0037] checking whether each of the first encoded data is the same as the second encoded data;

[0038] performing signature verification on the first data block and the first signed data of each of the transaction-related parties by using a public key of each of the transaction-related parties to verify whether the first data block matches the first signed data; and

[0039] performing signature verification on the second data block and the second signed data of the transaction initiator by using a public key of the transaction initiator to verify whether the second data block matches the second signed data; and

[0040] determining that check results of the checks are all Yes.

[0041] In one possible implementation, storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator comprises:

[0042] storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator in a block.

[0043] In a fourth aspect, a transaction processing apparatus is provided, the apparatus is deployed at a transaction initiator, comprising:

[0044] a sending unit, configured to send a transaction confirmation request for a target transaction to each transaction-related party, the transaction confirmation request comprising transaction data;

[0045] a receiving unit, configured to receive a transaction confirmation response from each of the transaction-related parties, the transaction confirmation response comprising a first data block and first signed data, wherein the first data block comprises first encoded data generated by encoding the transaction data

using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; and the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party;

[0046] an encoding unit, configured to encode the transaction data using the preset encoding method to generate second encoded data; and generate a second confirmation result;

[0047] a signing unit, configured to sign, by using a private key of the transaction initiator, a second data block comprising the second encoded data, the second confirmation result, and an identifier of the transaction initiator, so as to obtain second signed data; and

[0048] a storage unit, configured to store the first data block and the first signed data of each of the transaction-related parties that are received by the receiving unit and the second data block and the second signed data of the transaction initiator through a blockchain network, when it is determined that each of the first confirmation results received by the receiving unit and the second confirmation result generated by the encoding unit are Confirmed.

[0049] In a fifth aspect, a transaction processing apparatus is provided, the apparatus being deployed at a transaction-related party and comprising:

[0050] a receiving unit, configured to receive a transaction confirmation request for a target transaction from a transaction initiator, the transaction confirmation request comprising transaction data;

[0051] a confirmation unit, configured to generate a first confirmation result according to the transaction data received by the receiving unit;

[0052] an encoding unit, configured to encode the transaction data received by the receiving unit using a preset encoding method to generate first encoded data;

[0053] a signing unit, configured to sign, by using a private key of the transaction-related party, a first data block comprising the first confirmation result and the first encoded data, so as to obtain first signed data; and

[0054] a sending unit, configured to send a transaction confirmation response to the transaction initiator, the transaction confirmation response comprising the first data block and the first signed data, so that the transaction initiator stores the first data block and the first signed data of each of the transaction-related parties and data of the transaction initiator through a blockchain network when determining that a confirmation result of each of the transaction-related parties is Confirmed.

[0055] In a sixth aspect, a transaction processing apparatus is provided, the apparatus being deployed in a blockchain network and comprising:

[0056] a receiving unit, configured to receive, from a transaction initiator of a target transaction, a first data block and first signed data of each transaction-related party and a second data block and second signed data of the transaction initiator, wherein the first data block comprises first encoded data generated by encoding transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party; the second data block comprises second encoded data generated by encoding the transaction data using the preset encoding method by the transaction initiator, a second confirmation result, and an identifier of the transaction initiator; and the second signed data is obtained by performing signature computation on the second data block by using a private key of the transaction initiator; and

[0057] a storage unit, configured to store the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator that are received by the receiving unit.

[0058] In a seventh aspect, a computer-readable storage medium is provided, comprising a computer program stored thereon, wherein when executed in a computer, the computer program causes the computer to perform the method in the first aspect or the second aspect or the third aspect.

[0059] In an eighth aspect, a computing device is provided, comprising a memory and a processor, wherein the memory stores executable code, and when the processor executes the executable code, the method in the first aspect or the second aspect or the third aspect is implemented.

[0060] Through the method and apparatus provided in the embodiments of the present specification, a transaction initiator sends transaction data to a transaction-related party, thereby facilitating the transaction-related party in confirming the transaction, but the transaction-related party does not directly return the transaction data and a confirmation result to the transaction initiator; instead, the transaction-related party encodes the transaction data to obtain encoded data and returns the encoded data and the confirmation result to the transaction initiator, and subsequently, the transaction initiator does not directly store the transaction data and the confirmation result in a blockchain network, but stores the encoded data and the confirmation result as a data block in the blockchain network, and blockchain members do not know the transaction data, so that sensitive data is not leaked when the transaction data is stored using the blockchain network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0061] In order to illustrate the technical solutions in the embodiments of the present invention more clearly, the accompanying drawings required to be used in the description of the embodiments will be introduced briefly below. Apparently, the accompanying drawings described below are merely some embodiments of the present invention, and those of ordinary skill in the art can also obtain other accompanying drawings according to these accompanying drawings without making creative efforts.

[0062] FIG. 1 is a schematic diagram illustrating an implementation scenario of an embodiment disclosed in the present specification;

[0063] FIG. 2 is a schematic diagram illustrating a blockchain ledger implementation scenario corresponding to the implementation scenario shown in

FIG. 1;

[0064] FIG. 3 is a flowchart of a transaction processing method according to an embodiment;

[0065] FIG. 4 is a flowchart of a transaction processing method according to another embodiment;

[0066] FIG. 5 is a flowchart of a transaction processing method according to another embodiment;

[0067] FIG. 6 is a schematic diagram illustrating interactions among members during transaction processing according to an embodiment;

[0068] FIG. 7 is a sequence diagram of transaction processing according to an embodiment;

[0069] FIG. 8 is a schematic block diagram of a transaction processing apparatus according to an embodiment;

[0070] FIG. 9 is a schematic block diagram of a transaction processing apparatus according to another embodiment;

[0071] FIG. 10 is a schematic block diagram of a transaction processing apparatus according to another embodiment; and

[0072] FIG. 11 is a schematic block diagram of a transaction processing system according to an embodiment.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0073] The solutions provided in the present specification are described below with reference to the accompanying drawings.

[0074] FIG. 1 is a schematic diagram illustrating an implementation scenario of an embodiment disclosed in the present specification. The implementation scenario involves a fund transaction, which is specifically a transfer transaction. FIG. 1 illustrates a simplified transfer process, where Zhang San sends, through a first wallet, money to Li Si of a second wallet. Referring to FIG. 1, the flow direction of the fund is: first wallet (first member) → fund circulation bank (second member) → second wallet (third member). Blockchain

ledger is introduced in order to guarantee the reliability of fund flow, simplify reconciliation, shorten the transfer period, and so on.

[0075] FIG. 2 is a schematic diagram illustrating a blockchain ledger implementation scenario corresponding to the implementation scenario shown in FIG. 1. The implementation scenario involves data recording through a blockchain in a transfer process. Referring to FIG. 2, after joining the blockchain, a first member initiates a transaction through a first wallet, and the blockchain records transaction data and sends the recorded transaction data to all members. Financial regulation requires that each participant of a fund link needs to perform risk scanning, for example, anti-money laundering, anti-terrorism financing, etc. Such risk scanning often requires sensitive data (for example, an identity card number) of a user. Therefore, risk scanning needs to be initiated in the transaction process, and any one of the first member, a second member, and a third member may initiate risk scanning. The embodiment of the present specification merely uses the first member being a transaction initiator as an example for description, but it should be understood that the transaction initiator is not limited to the first member. After the first member initiates risk scanning, members in a fund link perform risk scanning and feed back scanning results. In order to prevent risks such as repudiation of individual members, detailed information and scanning results of risk scanning of the various members need to be written to the blockchain. However, the detailed information of risk scanning often contains a lot of privacy information, and such information will be leaked if written to the blockchain.

[0076] In view of the aforementioned problem, in the embodiment of the present specification, during transaction processing, transaction data stored on the blockchain after being encoded, thus realizing desensitization of transaction information, so that members on a transaction link approve the transaction and cannot repudiate the transaction, and do not leak the transaction information.

[0077] It should be noted that the implementation scenario involves a scenario in which multiple members participate in a blockchain transaction and

the members are required to approve the transaction. The multiple members may be only two members, for example, one transaction initiator and one transaction-related party; the multiple members may also be three or more members, for example, one transaction initiator and a plurality of transaction-related parties.

[0078] In addition, the transaction may be a fund transaction or may be a non-fund transaction.

[0079] For example, the non-fund transaction may be a car rental transaction. In the transaction, an intermediate party may not exist, the first member may be an intermediary/platform, and the second member is a rental company of a specific car provider. The first member submits information of an actual renter in plaintext to the second member for confirming whether renting can be performed, and then the second member encodes the information and signs the encoded data and a confirmation result together and returns them to the first member. Finally, the first member places the desensitized information on the blockchain.

[0080] It can be understood that the transaction processing method in the embodiment of the present specification can be applied to many implementation scenarios, as long as multiple members participate in a blockchain transaction and the members are required to approve the transaction, which will not be described herein again.

[0081] FIG. 3 is a flowchart of a transaction processing method according to an embodiment. The method is performed by a transaction initiator, for example, the first member in the scenario shown in FIG. 2. As shown in FIG. 3, the transaction processing method in the embodiment includes the following steps: step 31: sending a transaction confirmation request for a target transaction to each transaction-related party, the transaction confirmation request including transaction data; step 32: receiving a transaction confirmation response from each of the transaction-related parties, the transaction confirmation response including a first data block and first signed data, wherein the first data block includes first encoded data generated by encoding the transaction data using a preset encoding

method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; and the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party; step 33: encoding the transaction data using the preset encoding method to generate second encoded data; and generating a second confirmation result; step 34: signing, by using a private key of the transaction initiator, a second data block including the second encoded data, the second confirmation result, and an identifier of the transaction initiator, so as to obtain second signed data; and step 35: storing the first data block and the first signed data of each of the transaction-related parties and a second data block and second signed data of the transaction initiator through a blockchain network when determining that each of the first confirmation results and the second confirmation result are Confirmed. The specific execution method of the aforementioned steps is described below.

[0082] First, at step 31, a transaction confirmation request for a target transaction is sent to each transaction-related party, the transaction confirmation request including transaction data.

[0083] In embodiment of the present specification, the content of the transaction data is not limited. For example, the transaction data may include but is not limited to privacy information of a user, such as the name, identity card number, age etc.

[0084] Next, at step 32: a transaction confirmation response from each of the transaction-related parties is received, the transaction confirmation response including a first data block and first signed data, where the first data block includes first encoded data generated by encoding the transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; and the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party.

[0085] It can be understood that the number of the transaction-related parties may be multiple or may be one.

[0086] The preset encoding method may be any encoding method in which original data cannot be easily obtained by encoding the data, for example, a hash encoding method.

[0087] The first confirmation result is used for indicating whether the transaction-related party approves the target transaction.

[0088] The signed data can be used for proving the identity, each member of the blockchain has a member ID and a pair of public and private keys, where the public key is public, and the public and private keys can be used for proving the identity. For example, A may sign data D using a private key to obtain a signature string S; A sends data D and signature string S to B; B performs signature verification on data D and signature string S through a public key of A, and if they match, it indicates that the data received by B really comes from A.

[0089] Afterwards, at step 33, the transaction data is encoded using the preset encoding method to generate second encoded data; and a second confirmation result is generated.

[0090] It can be understood that the transaction initiator and the transaction-related party have the same manner of generating encoded data; theoretically, the first encoded data and the second encoded data should also be the same, and whether they are the same may be subsequently checked by the blockchain network.

[0091] The second confirmation result is used for indicating whether the transaction initiator approves the target transaction.

[0092] Then, at step 34, by using a private key of the transaction initiator, a second data block including the second encoded data, the second confirmation result, and an identifier of the transaction initiator is signed, so as to obtain second signed data.

[0093] The manner of the signature computation has been described previously, and will not be described herein again.

[0094] Finally, at step 35, the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator are stored through the blockchain network, when it is determined that each of the first confirmation results and the second confirmation result are Confirmed.

[0095] In an example, the target transaction may further be processed through the blockchain network when it is determined that each of the first confirmation results and the second confirmation result are Confirmed. For example, processing result information of the target transaction is recorded through the blockchain network; and the processing result information of the target transaction is sent to each of the transaction-related parties through the blockchain network, so that each of the transaction-related parties processes the target transaction.

[0096] Through the method provided in the embodiment of the present specification, a transaction initiator sends transaction data to a transaction-related party, thereby facilitating the transaction-related party in confirming the transaction, but the transaction-related party does not directly return the transaction data and a confirmation result to the transaction initiator; instead, the transaction-related party encodes the transaction data to obtain encoded data and returns the encoded data and the confirmation result to the transaction initiator, and subsequently, the transaction initiator does not directly store the transaction data and the confirmation result in a blockchain network, but stores the encoded data and the confirmation result as a data block in the blockchain network, and blockchain members do not know the transaction data, so that sensitive data is not leaked when the transaction data is stored using the blockchain network.

[0097] FIG. 4 is a flowchart of a transaction processing method according to another embodiment. The method is performed by a transaction-related party, for example, the second member or the third member in the scenario shown in FIG. 2. As shown in FIG. 4, the transaction processing method in the embodiment includes the following steps: step 41: receiving a transaction

confirmation request for a target transaction from a transaction initiator, the transaction confirmation request including transaction data; step 42: generating a first confirmation result according to the transaction data; step 43: encoding the transaction data using a preset encoding method to generate first encoded data; step 44: signing, by using a private key of the transaction-related party, a first data block including the first confirmation result and the first encoded data, so as to obtain first signed data; and step 45: sending a transaction confirmation response to the transaction initiator, the transaction confirmation response including the first data block and the first signed data, so that the transaction initiator stores the first data block and the first signed data of each of the transaction-related parties and data of the transaction initiator through a blockchain network when determining that a confirmation result of each of the transaction-related parties is Confirmed. The specific execution method of the aforementioned steps is described below.

[0098] First, at step 41, a transaction confirmation request for a target transaction from a transaction initiator is received, the transaction confirmation request including transaction data.

[0099] In the embodiment of the present specification, the content of the transaction data is not limited. For example, the transaction data may include but is not limited to privacy information of a user, such as the name, identity card number, age etc.

[00100] Next, at step 42, a first confirmation result according to the transaction data is generated.

[00101] The first confirmation result is used for indicating whether the transaction-related party approves the target transaction.

[00102] Afterwards, at step 43: the transaction data is encoded using a preset encoding method to generate first encoded data.

[00103] It can be understood that the transaction initiator and the transaction-related party have the same manner of generating encoded data; theoretically, the first encoded data and the second encoded data should also be

the same, and whether they are the same may be subsequently checked by the blockchain network.

[00104] Then, at step 44, by using a private key of the transaction-related party, a first data block including the first confirmation result and the first encoded data is signed, so as to obtain first signed data.

[00105] The manner of the signature computation has been described previously, and will not be described herein again.

[00106] Finally, at step 45, a transaction confirmation response is sent to the transaction initiator, the transaction confirmation response including the first data block and the first signed data, so that the transaction initiator stores the first data block and the first signed data of each of the transaction-related parties and data of the transaction initiator through a blockchain network when determining that a confirmation result of each of the transaction-related parties is Confirmed.

[00107] The data of the transaction initiator includes the second data block and the second signed data of the transaction initiator. Reference may be made to the corresponding description in FIG. 3 for details.

[00108] In an example, the method further includes:

[00109] receiving processing result information of the target transaction from the blockchain network; and

[00110] processing the target transaction according to the processing result information.

[00111] Through the method provided in the embodiment of the present specification, a transaction-related party receives transaction data from a transaction initiator, thereby facilitating the transaction-related party in confirming the transaction, but the transaction-related party does not directly return the transaction data and a confirmation result to the transaction initiator; instead, the transaction-related party encodes the transaction data to obtain encoded data and returns the encoded data and the confirmation result to the transaction initiator, and subsequently, the transaction initiator does not directly store the transaction data and the confirmation result in a blockchain network, but

stores the encoded data and the confirmation result as a data block in the blockchain network, and blockchain members do not know the transaction data, so that sensitive data is not leaked when the transaction data is stored using the blockchain network.

[00112] FIG. 5 is a flowchart of a transaction processing method according to another embodiment. The method is performed by a blockchain network, and the blockchain network may be called a blockchain for short, for example, the blockchain in the scenario shown in FIG. 2. As shown in FIG. 5, the transaction processing method in the embodiment includes the following steps:

[00113] step 51: receive, from a transaction initiator of a target transaction, a first data block and first signed data of each transaction-related party and a second data block and second signed data of the transaction initiator, where the first data block includes first encoded data generated by encoding transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party; the second data block includes second encoded data generated by encoding the transaction data using the preset encoding method by the transaction initiator, a second confirmation result, and an identifier of the transaction initiator; and the second signed data is obtained by performing signature computation on the second data block by using a private key of the transaction initiator.

[00114] It can be understood that the transaction initiator and the transaction-related party may join the blockchain network in advance to become members of the blockchain network.

[00115] Step 52: store the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator.

[00116] In an example, after step 52, the method may further include processing the target transaction. For example, processing result information of

the target transaction is recorded; and the processing result information of the target transaction is sent to each of the transaction-related parties, so that each of the transaction-related parties processes the target transaction.

[00117] In an example, before step 52, the method may further include:

[00118] performing the following checks:

[00119] checking whether the identifier of the transaction-related party and/or the identifier of the transaction initiator matches a member identifier on a transaction link of the target transaction;

[00120] checking whether each of the first encoded data is the same as the second encoded data;

[00121] performing signature verification on the first data block and the first signed data of each of the transaction-related parties by using a public key of each of the transaction-related parties to verify whether the first data block matches the first signed data; and

[00122] performing signature verification on the second data block and the second signed data of the transaction initiator by using a public key of the transaction initiator to verify whether the second data block matches the second signed data; and

[00123] determining that check results of the checks are all Yes.

[00124] As an example, step 52 may be specifically storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator in a block.

[00125] Through the method provided in the embodiment of the present specification, a blockchain network does not directly receive transaction data and a confirmation result from a transaction initiator, but receives encoded data and the confirmation result and stores the encoded data and the confirmation result as a data block in the blockchain network, and blockchain members do not know the transaction data, so that sensitive data is not leaked when the transaction data is stored using the blockchain network.

[00126] FIG. 6 is a schematic diagram illustrating interactions among members during transaction processing according to an embodiment. FIG. 7 is a sequence diagram of transaction processing according to an embodiment. Referring to FIG. 6 or FIG. 7, a transaction link involves a first member, a second member, and a third member, where the first member is a transaction initiator, the second member and the third member are transaction-related parties, and the conduction of a transaction needs to obtain approval of the first member, the second member, and the third member.

[00127] In an embodiment according to another aspect, a transaction processing apparatus is further provided, the apparatus being deployed at a transaction initiator. FIG. 8 is a schematic block diagram of a transaction processing apparatus according to an embodiment. As shown in FIG. 8, the apparatus 800 includes:

[00128] a sending unit 81, configured to send a transaction confirmation request for a target transaction to each transaction-related party, the transaction confirmation request including transaction data;

[00129] a receiving unit 82, configured to receive a transaction confirmation response from each of the transaction-related parties, the transaction confirmation response including a first data block and first signed data, wherein the first data block includes first encoded data generated by encoding the transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; and the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party;

[00130] an encoding unit 83, configured to encode the transaction data using the preset encoding method to generate second encoded data; and generate a second confirmation result;

[00131] a signing unit 84, configured to sign, by using a private key of the transaction initiator, a second data block including the second encoded data, the second confirmation result, and an identifier of the transaction initiator, so as to

obtain second signed data; and

[00132] a storage unit 85, configured to store, through a blockchain network, the first data block and the first signed data of each of the transaction-related parties that are received by receiving unit 82 and the second data block and the second signed data of the transaction initiator, when it is determined that each of the first confirmation results received by receiving unit 82 and the second confirmation result generated by encoding unit 83 are Confirmed.

[00133] Optionally, as an embodiment, the apparatus further includes:

[00134] a processing unit, configured to process the target transaction through the blockchain network when it is determined that each of the first confirmation results received by receiving unit 82 and the second confirmation result are Confirmed.

[00135] Further, the processing unit is specifically configured to:

[00136] record processing result information of the target transaction through the blockchain network; and

[00137] send the processing result information of the target transaction to each of the transaction-related parties through the blockchain network, so that each of the transaction-related parties processes the target transaction.

[00138] Through the apparatus provided in the embodiment of the present specification, sending unit 81 sends transaction data to a transaction-related party, thereby facilitating the transaction-related party in confirming the transaction, but the transaction-related party does not directly return the transaction data and a confirmation result to receiving unit 82; instead, the transaction-related party encodes the transaction data to obtain encoded data and returns the encoded data and the confirmation result to receiving unit 82, and subsequently, storage unit 85 does not directly store the transaction data and the confirmation result in a blockchain network, but stores the encoded data and the confirmation result as a data block in the blockchain network, and blockchain members do not know the transaction data, so that sensitive data is not leaked when the transaction data is stored using the blockchain network.

[00139] In an embodiment according to another aspect, a transaction processing apparatus is further provided, the apparatus being deployed at a transaction-related party. FIG. 9 is a schematic block diagram of a transaction processing apparatus according to another embodiment. As shown in FIG. 9, apparatus 900 includes:

[00140] a receiving unit 91, configured to receive a transaction confirmation request for a target transaction from a transaction initiator, the transaction confirmation request including transaction data;

[00141] a confirmation unit 92, configured to generate a first confirmation result according to the transaction data received by receiving unit 91;

[00142] an encoding unit 93, configured to encode the transaction data received by receiving unit 91 using a preset encoding method to generate first encoded data;

[00143] a signing unit 94, configured to sign, by using a private key of the transaction-related party, a first data block including the first confirmation result and the first encoded data, so as to obtain first signed data; and

[00144] a sending unit 95, configured to send a transaction confirmation response to the transaction initiator, the transaction confirmation response including the first data block and the first signed data, so that the transaction initiator stores the first data block and the first signed data of each of the transaction-related parties and data of the transaction initiator through a blockchain network when determining that a confirmation result of each of the transaction-related parties is Confirmed.

[00145] Optionally, as an embodiment,

[00146] receiving unit 91 is further configured to receive processing result information of the target transaction from the blockchain network; and

[00147] the apparatus further includes:

[00148] a processing unit, configured to process the target transaction according to the processing result information received by receiving unit 91.

[00149] Through the apparatus provided in the embodiment of the present specification, receiving unit 91 receives transaction data from a transaction initiator, thereby facilitating confirmation unit 92 in confirming the transaction, but sending unit 95 does not directly return the transaction data and a confirmation result to the transaction initiator; instead, the transaction-related party encodes the transaction data to obtain encoded data and returns the encoded data and the confirmation result to the transaction initiator, and subsequently, the transaction initiator does not directly store the transaction data and the confirmation result in a blockchain network, but stores the encoded data and the confirmation result as a data block in the blockchain network, and blockchain members do not know the transaction data, so that sensitive data is not leaked when the transaction data is stored using the blockchain network.

[00150] In an embodiment according to another aspect, a transaction processing apparatus is further provided, the apparatus being deployed in a blockchain network, and specifically, deployed on a node of the blockchain network, which may be called a blockchain for short. FIG. 10 is a schematic block diagram of a transaction processing apparatus according to another embodiment. As shown in FIG. 10, apparatus 1000 includes:

[00151] a receiving unit 1001, configured to receive, from a transaction initiator of a target transaction, a first data block and first signed data of each transaction-related party and a second data block and second signed data of the transaction initiator, wherein the first data block includes first encoded data generated by encoding transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party; the second data block includes second encoded data generated by encoding the transaction data using the preset encoding method by the transaction initiator, a second confirmation result, and an identifier of the transaction initiator; and the second signed data is obtained by performing signature computation on

the second data block by using a private key of the transaction initiator; and

[00152] a storage unit 1002, configured to store the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator that are received by receiving unit 1001.

[00153] Optionally, as an embodiment, the apparatus further includes:

[00154] a processing unit, configured to process the target transaction after storage unit 1002 stores the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator.

[00155] Further, the processing unit is specifically configured to:

[00156] record processing result information of the target transaction; and

[00157] send the processing result information of the target transaction to each of the transaction-related parties, so that each of the transaction-related parties processes the target transaction.

[00158] Further, the apparatus further includes:

[00159] a checking unit, configured to perform the following checks before storage unit 1002 stores the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator:

[00160] checking whether the identifier of the transaction-related party and/or the identifier of the transaction initiator matches a member identifier on a transaction link of the target transaction;

[00161] checking whether each of the first encoded data is the same as the second encoded data;

[00162] performing signature verification on the first data block and the first signed data of each of the transaction-related parties by using a public key of each of the transaction-related parties to verify whether the first data block matches the first signed data; and

[00163] performing signature verification on the second data block and the second signed data of the transaction initiator by using a public key of the transaction initiator to verify whether the second data block matches the second signed data; and

[00164] a determining unit, configured to determine that checking results of the checks obtained by the checking unit are all Yes.

[00165] Optionally, as an embodiment, storage unit 1002 is specifically configured to store, in a block, the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator that are received by receiving unit 1001.

[00166] Through the apparatus provided in the embodiment of the present specification, receiving unit 1001 does not directly receive transaction data and a confirmation result from a transaction initiator, but receives encoded data and the confirmation result, and storage unit 1002 stores the encoded data and the confirmation result as a data block in a blockchain network, and blockchain members do not know the transaction data, so that sensitive data is not leaked when the transaction data is stored using the blockchain network.

[00167] In an embodiment according to another aspect, a transaction processing system is further provided, the system including a first member transaction system, a second member transaction system, blockchain bridging systems, and a blockchain. FIG. 11 is a schematic block diagram of a transaction processing system according to an embodiment. As shown in FIG. 11, the processing process of the system includes:

[00168] First, a first member (i.e., a transaction initiator) initiates a transaction confirmation request to a blockchain bridging system of the first member, where data in the request includes detail data agreed upon in a transaction (hereinafter collectively referred to as BIZ_DATA).

[00169] Next, after a receiving module of the blockchain bridging system of the first member receives the request, the data is sent to all members on a transaction link in an agreed format by a sending module, where the sent data

includes BIZ_DATA.

[00170] Afterwards, after receiving the request, a receiving module of a blockchain bridging system of a second member (if transaction-related parties further include a third member, the third member uses the same processing logic as the second member) forwards the data to the second member's transaction system to perform transaction confirmation, where the received data includes BIZ_DATA. After performing confirmation, the second member returns a confirmation result (hereinafter collectively referred to as RESULT) to the receiving module of the blockchain bridging system. The receiving module transfers the BIZ_DATA and the result to a desensitization module for processing.

[00171] Then, the desensitization module of the blockchain bridging system of the second member performs hash processing (other encoding methods may also be adopted) on the BIZ_DATA to calculate a corresponding hash code. Then, the hash code and RESULT are transferred to a signing module.

[00172] Afterwards, the signing module of the blockchain bridging system of the second member uses the hash code, RESULT, and a preset member ID of the second member as a data block (hereinafter collectively referred to as CHECK_RESULT) according to an agreed format, and then calculates a signature (hereinafter collectively referred to as SIGNATURE) using a private key.

[00173] Then, a sending module of the blockchain bridging system of the second member returns the CHECK_RESULT and SIGNATURE to the first member.

[00174] Then, after receiving CHECK_RESULT and SIGNATURE returned by all members on the transaction link, the sending module of the blockchain bridging system of the first member parses and examines transaction confirmation results (the RESULT) in all of the received CHECK_RESULT to see whether they are all Confirmed, and if yes, an access module is further invoked.

[00175] Then, the access module of the blockchain bridging system of the first member sends CHECK_RESULT and SIGNATURE of all the members on the transaction link to the blockchain for processing.

[00176] Then, a checking module in the blockchain performs the following checks: parsing all CHECK_RESULT, where parsed data includes the hash codes, RESULT, and member IDs; checking whether all the parsed member IDs match all the member IDs on the transaction link; checking whether the hash codes of every members are completely the same; examining each pair of CHECK_RESULT and SIGNATURE, obtaining a public key of a corresponding member through a member ID, and performing signature verification on CHECK_RESULT and SIGNATURE using the public to verify whether they match.

[00177] Finally, the blockchain can invoke a transaction module of the blockchain to perform transaction processing after the checks are all completed.

[00178] In an embodiment according to another aspect, a computer-readable storage medium is further provided, having a computer program stored thereon, where when executed in a computer, the computer program causes the computer to perform the method described with reference to any one of FIG. 3 to FIG. 5.

[00179] In an embodiment according to yet another aspect, a computing device is further provided, including a memory and a processor, where the memory stores executable code, and when the processor executes the executable code, the method described with reference to any one of FIG. 3 to FIG. 5 is implemented.

[00180] Those skilled in the art should realize that in the aforementioned one or plurality of examples, the functions described in the present invention may be implemented by hardware, software, or firmware, or any combination thereof. When implemented by software, these functions may be stored in a computer-readable medium, or transmitted as one or a plurality of instructions or as one or a plurality of pieces of code in the computer-readable medium.

[00181] The objectives, the technical solutions, and the beneficial effects of the present invention are further described in detail in the foregoing specific implementation. It should be understood that the foregoing descriptions are merely specific implementation of the present invention, and are not intended to limit the protection scope of the present invention. Any modification, equivalent replacement, and improvement made on the basis of the technical solutions of the present invention shall fall within the protection scope of the present invention.

What Is Claimed Is

1. A transaction processing method, the method being performed by a transaction initiator and comprising:

sending a transaction confirmation request for a target transaction to each transaction-related party, the transaction confirmation request comprising transaction data;

receiving a transaction confirmation response from each of the transaction-related parties, the transaction confirmation response comprising a first data block and first signed data, wherein the first data block comprises first encoded data generated by encoding the transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party, and the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party;

encoding the transaction data using the preset encoding method to generate second encoded data; and generating a second confirmation result;

signing, by using a private key of the transaction initiator, a second data block comprising the second encoded data, the second confirmation result, and an identifier of the transaction initiator, so as to obtain second signed data; and

storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator through a blockchain network when determining that each of the first confirmation results and the second confirmation result are Confirmed.

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

processing the target transaction through the blockchain network when determining that each of the first confirmation results and the second confirmation result are Confirmed.

3. The method according to claim 2, wherein processing the target transaction through the blockchain network comprises:

recording processing result information of the target transaction through the blockchain network; and

sending the processing result information of the target transaction to each of the transaction-related parties through the blockchain network, so that each of the transaction-related parties processes the target transaction.

4. A transaction processing method, the method being performed by a transaction-related party and comprising:

receiving a transaction confirmation request for a target transaction from a transaction initiator, the transaction confirmation request comprising transaction data;

generating a first confirmation result according to the transaction data;

encoding the transaction data using a preset encoding method to generate first encoded data;

signing, by using a private key of the transaction-related party, a first data block comprising the first confirmation result and the first encoded data, so as to obtain first signed data; and

sending a transaction confirmation response to the transaction initiator, the transaction confirmation response comprising the first data block and the first signed data, so that the transaction initiator stores the first data block and the first signed data of each of the transaction-related parties and data of the transaction initiator through a blockchain network when determining that a confirmation result of each of the transaction-related parties is Confirmed.

5. The method according to claim 4, further comprising:

receiving processing result information of the target transaction from the blockchain network; and

processing the target transaction according to the processing result information.

6. A transaction processing method, the method being performed by a blockchain network and comprising:

receiving, from a transaction initiator of a target transaction, a first data block and first signed data of each transaction-related party and a second data block and second signed data of the transaction initiator, wherein the first data block comprises first encoded data generated by encoding transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party; the second data block comprises second encoded data generated by encoding the transaction data using the preset encoding method by the transaction initiator, a second confirmation result, and an identifier of the transaction initiator; and the second signed data is obtained by performing signature computation on the second data block by using a private key of the transaction initiator; and

storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator.

7. The method according to claim 6, wherein, after storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator, the

method further comprises:

processing the target transaction.

8. The method according to claim 7, wherein processing the target transaction comprises:

recording processing result information of the target transaction; and

sending the processing result information of the target transaction to each of the transaction-related parties, so that each of the transaction-related parties processes the target transaction.

9. The method according to claim 7, wherein, before storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator, the method further comprises:

performing the following checks:

checking whether the identifier of the transaction-related party and/or the identifier of the transaction initiator matches a member identifier on a transaction link of the target transaction;

checking whether each of the first encoded data is the same as the second encoded data;

performing signature verification on the first data block and the first signed data of each of the transaction-related parties by using a public key of each of the transaction-related parties to verify whether the first data block matches the first signed data; and

performing signature verification on the second data block and the second signed data of the transaction initiator by using a public key of the transaction initiator to verify whether the second data block matches the second signed data; and

determining that checking results of the checks are all Yes.

10. The method according to claim 6, wherein storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator comprises:

storing the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator in a block.

11. A transaction processing apparatus, the apparatus being deployed at a transaction initiator and comprising:

a sending unit, configured to send a transaction confirmation request for a target transaction to each transaction-related party, the transaction confirmation request comprising transaction data;

a receiving unit, configured to receive a transaction confirmation response from each of the transaction-related parties, the transaction confirmation response comprising a first data block and first signed data, wherein the first data block comprises first encoded data generated by encoding the transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; and the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party;

an encoding unit, configured to encode the transaction data using the preset encoding method to generate second encoded data; and generate a second confirmation result;

a signing unit, configured to sign, by using a private key of the transaction initiator, a second data block comprising the second encoded data, the second confirmation result, and an identifier of the transaction initiator, so as to obtain second signed data; and

a storage unit, configured to store the first data block and the first signed data of each of the transaction-related parties that are received by the receiving unit and the second data block and the second signed data of the transaction initiator through a blockchain network, when it is determined that each of the first confirmation results received by the receiving unit and the second confirmation result generated by the encoding unit are Confirmed.

12. The apparatus according to claim 11, further comprising:

a processing unit, configured to process the target transaction through the blockchain network when it is determined that each of the first confirmation results received by the receiving unit and the second confirmation result are Confirmed.

13. The apparatus according to claim 12, wherein the processing unit is specifically configured to:

record processing result information of the target transaction through the blockchain network; and

send the processing result information of the target transaction to each of the transaction-related parties through the blockchain network, so that each of the transaction-related parties processes the target transaction.

14. A transaction processing apparatus, the apparatus being deployed at a transaction-related party and comprising:

a receiving unit, configured to receive a transaction confirmation request for a target transaction from a transaction initiator, the transaction confirmation request comprising transaction data;

a confirmation unit, configured to generate a first confirmation result according to the transaction data received by the receiving unit;

an encoding unit, configured to encode the transaction data received by the

receiving unit using a preset encoding method to generate first encoded data;

a signing unit, configured to sign, by using a private key of the transaction-related party, a first data block comprising the first confirmation result and the first encoded data, so as to obtain first signed data; and

a sending unit, configured to send a transaction confirmation response to the transaction initiator, the transaction confirmation response comprising the first data block and the first signed data, so that the transaction initiator stores the first data block and the first signed data of each of the transaction-related parties and data of the transaction initiator through a blockchain network when determining that a confirmation result of each of the transaction-related parties is Confirmed.

15. The apparatus according to claim 14, wherein:

the receiving unit is further configured to receive processing result information of the target transaction from the blockchain network; and

the apparatus further comprises:

a processing unit, configured to process the target transaction according to the processing result information received by the receiving unit.

16. A transaction processing apparatus, the apparatus being deployed in a blockchain network and comprising:

a receiving unit, configured to receive, from a transaction initiator of a target transaction, a first data block and first signed data of each transaction-related party and a second data block and second signed data of the transaction initiator, wherein the first data block comprises first encoded data generated by encoding transaction data using a preset encoding method by the transaction-related party, a first confirmation result, and an identifier of the transaction-related party; the first signed data is obtained by performing signature computation on the first data block by using a private key of the transaction-related party; the second data block comprises second encoded data generated by

encoding the transaction data using the preset encoding method by the transaction initiator, a second confirmation result, and an identifier of the transaction initiator; and the second signed data is obtained by performing signature computation on the second data block by using a private key of the transaction initiator; and

a storage unit, configured to store the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator that are received by the receiving unit.

17. The apparatus according to claim 16, further comprising:

a processing unit, configured to process the target transaction after the storage unit stores the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator.

18. The apparatus according to claim 17, wherein the processing unit is specifically configured to:

record processing result information of the target transaction; and

send the processing result information of the target transaction to each of the transaction-related parties, so that each of the transaction-related parties processes the target transaction.

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

a checking unit, configured to perform the following checks before the storage unit stores the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator:

checking whether the identifier of the transaction-related party and/or the identifier of the transaction initiator matches a member identifier on a transaction

link of the target transaction;

checking whether each of the first encoded data is the same as the second encoded data;

performing signature verification on the first data block and the first signed data of each of the transaction-related parties by using a public key of each of the transaction-related parties to verify whether the first data block matches the first signed data; and

performing signature verification on the second data block and the second signed data of the transaction initiator by using a public key of the transaction initiator to verify whether the second data block matches the second signed data; and

a determining unit, configured to determine that checking results of the checks obtained by the check unit are all Yes.

20. The apparatus according to claim 16, wherein the storage unit is specifically configured to store, in a block, the first data block and the first signed data of each of the transaction-related parties and the second data block and the second signed data of the transaction initiator that are received by the receiving unit.

21. A computer-readable storage medium, having a computer program stored thereon, wherein when executed in a computer, the computer program causes the computer to perform the method according to any one of claims 1 to 10.

22. A computing device, comprising a memory and a processor, wherein the memory stores executable code, and when the processor executes the executable code, the method according to any one of claims 1 to 10 is implemented.