

TRANSACTION PROCESSING METHOD, DEVICE, COMPUTER EQUIPMENT AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] The present disclosure relates to the field of blockchain technology, and particularly to a transaction processing method and apparatus, a computer equipment and a storage medium.

BACKGROUND

[0002] With the development of blockchain technology, the demand for data security on the chain is increasing. Hyperledger Fabric is the current mainstream blockchain system platform. Commercial transactions often involve some private data which can't be viewed by all the peers on the chain. How to achieve private data protection in transactions is a major problem that needs to be resolved at present.

[0003] At present, channels are used in Hyperledger Fabric to protect private data. Data in different channels are isolated from each other, and members outside the channel cannot access the information in the channel, thereby achieving transaction private. When some members in a channel need to ensure the private of the data and prevent other members in the channel from accessing it, these members can create a channel separately, which contains only members who have permission to read these private data. However, in order to achieve private data protection, creating a large number of channels in a large network and storing the data in different channels will bring additional overhead, such as management strategies, chaincode versions, and Membership Service Provider (MSP). Therefore, private transactions have been introduced in Hyperledger Fabric, allowing private data sets to be created based on policies to define which members of the channel can access the data.

[0004] However, in the current private transaction process, the private data is stored in the local temporary storage area of the authorized peer in clear text based on the data set policy. Once the policy has a loophole and is tampered with, or a malicious peer

obtains the permission, it can access private data in plaintext that will cause security risks.

SUMMARY

[0005] Based on this, it is necessary to provide a transaction processing method, device, computer equipment, and storage medium that can improve the security of private data in response to the above technical problems.

[0006] A transaction processing method, which is applied to the client terminal, includes:

[0007] The client responds to the transaction request and obtains identification information and private data corresponding to the transaction request;

[0008] The client calls the encryption key management contract, generates a key according to the identification information, and uses the generated key to encrypt private data to obtain encrypted private data;

[0009] The client sends a transaction proposal to the endorsing peer, and the transaction proposal includes identification information and encrypted private data; the encryption key management contract is called by the endorsing peer, the corresponding key is obtained according to the identification information, and the obtained key is used to decrypt the encrypted private data, and simulate the transaction to generate the transaction read-write set. Finally, the endorsing peer sends a transaction read-write set to a randomly selected committing peer among the authorized peers that have the right to access private data;

[0010] The client receives the proposal response returned by the endorsing peer. The proposal response includes the transaction read-write set, which sends transaction information to the ordering peer, and the transaction information includes the transaction read-write set and transaction proposal; The ordering peer generates a block according to the transaction information, and sends the block to the committing peer; the committing

peer verifies the validity of the transaction based on the block and the transaction read-write set received from the endorsing peer.

[0011] A transaction processing device, which is applied to the client, includes:

[0012] An acquisition module is used to obtain identification information and private data corresponding to the transaction request in response to the transaction request;

[0013] An encryption module is used to call an encryption key management contract, generate a key according to the identification information, and use the generated key to encrypt the private data to obtain encrypted private data;

[0014] A sending module is used to send a transaction proposal to the endorsing peer, the transaction proposal includes the identification information and the encrypted private data; the endorsing peer calls the encryption key management contract, and obtains the corresponding key, and uses the obtained key to decrypt the encrypted private data, simulates a transaction to generate a transaction read-write set, and sends the transaction read-write set to the committing peer randomly selected among the authorized peers that have access to the private data;

[0015] A receiving module, configured to receive a proposal response returned by the endorsing peer, where the proposal response includes the transaction read-write set;

[0016] A sending module is also used to send transaction information to the ordering peer, the transaction information includes the transaction read-write set and the transaction proposal; the ordering peer generates a block according to the transaction information, and sends it to the committing peer; the committing peer verifies the validity of the transaction based on the block and the transaction read-write set received from the endorsing peer.

[0017] A transaction processing method, which is applied to the endorsing peer, includes:

[0018] The endorsing peer obtains a transaction proposal sent by the client, the

transaction proposal includes identification information and encrypted private data, and the client responds to the transaction request to obtain the identification information and private data corresponding to the transaction request; calls an encryption key management contract, generates a key according to the identification information, and encrypts the private data with the generated key;

[0019] The endorsing peer calls the encryption key management contract, obtains the corresponding key according to the identification information, and uses the obtained key to decrypt the encrypted private data, simulates a transaction to generate a transaction read-write set, and sends the transaction read-write set to the committing peer randomly selected among the authorized peers that have access to the private data;

[0020] The endorsing peer returns a proposal response to the client, the proposal response includes the transaction read-write set; the client sends the transaction information to the ordering peer, the transaction information includes the transaction read-write set and the transaction proposal; the ordering peer generates a block according to the transaction information, and sends the block to the verification peer; the verification peer reads the block according to the block and the transaction received from the endorsing peer to verify the validity of the transaction.

[0021] A transaction processing device, which is applied to the endorsing peer, includes:

[0022] An obtaining module is used to obtain the transaction proposal sent by the client. The transaction proposal includes identification information and encrypted private data. The client responds to the transaction request to obtain the transaction request corresponding to the encrypted private data. The endorsing peer identify information and private data, call an encryption key management contract, generate a key according to the identification information, and encrypt the private data using the generated key;

[0023] A processing module is used to call the encryption key management contract, obtain the corresponding key according to the identification information, and use the obtained key to decrypt the encrypted private data, simulate a transaction to

generate a transaction read-write set, the committing peer is randomly selected among the authorized peers to access private data sends the transaction read-write set;

[0024] A return module is configured to return a proposal response to the client, the proposal response includes the transaction read-write set; the client sends the transaction information to the ordering peer, the transaction information includes the transaction read-write set and the transaction proposal; the ordering peer generates a block based on the transaction information, and sends the block to the committing peer; the committing peer based on the block and the transaction read and write set received from the endorsing peer to verify the validity of the transaction.

[0025] A transaction processing method, which is applied to the committing peer, includes:

[0026] The committing peer receives the transaction read-write set sent by the endorsing peer; the transaction read-write set is obtained by the endorsing peer including the identification information and the encrypted private data transaction proposal sent by the client, calls the encryption key management contract, and obtains the corresponding according to the identification information and use the obtained key to decrypt the encrypted private data to simulate transaction generation; the client responds to the transaction request to obtain the identification information and the corresponding identification information of the encrypted private data private data, calling an encryption key management contract, generating a key according to the identification information, and encrypting the private data with the generated key;

[0027] The committing peer obtains the block sent by the ordering peer; the block is generated by the ordering peer according to the transaction information received from the client, the transaction information includes the transaction proposal and the proposal response returned by the endorsing peer transaction read-write set;

[0028] According to the block and the transaction read-write set received from the endorsing peer, the validity of the transaction is verified.

[0029] A transaction processing device, which is applied to the committing peer,

includes:

[0030] A receiving module is used to receive the transaction read-write set sent by the endorsing peer; the transaction read-write set is obtained by the endorsing peer including the identification information and the encrypted private data transaction proposal sent by the client, call the encryption key management contract, and obtains the corresponding according to the identification information and use the obtained key to decrypt the encrypted private data to simulate transaction generation; the client responds to the transaction request to obtain the identification information and the corresponding identification information of the encrypted private data private data, calling an encryption key management contract, generating a key according to the identification information, and encrypting the private data with the generated key;

[0031] An obtaining module is used to obtain the block sent by the ordering peer; the block is generated by the ordering peer according to the transaction information received from the client, the transaction information includes the transaction proposal and the proposal response returned by the endorsing peer transaction read-write set;

[0032] A committing module is used to verify the validity of the transaction according to the block and the transaction read-write set received from the endorsing peer.

[0033] A computer device includes a memory and a processor, the memory stores a computer program, and the processor implements the steps of the transaction processing method when the computer program is executed.

[0034] A computer-readable storage medium has a computer program stored thereon, and when the computer program is executed by a processor, the steps of the transaction processing method are realized.

[0035] The above transaction processing method, device, computer equipment and storage medium use the encryption key management contract to set the access authority of the private data in the transaction, ensure that the private data is only visible to the authorized peers, and use the encryption key management contract to generate the key to

encrypt the private data , so that private data is transmitted in ciphertext form, and the private data stored by authorized peers is not in plaintext form, which can avoid data leakage caused by malicious access and improve the security of private data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0036] FIG.1 is an application environment diagram of a transaction processing method in an embodiment;

[0037] FIG.2 is a schematic flow chart of a transaction processing method in an embodiment;

[0038] FIG.3 is a schematic flowchart of a transaction processing method in an embodiment;

[0039] FIG.4 is a schematic flow chart of a transaction processing method in an embodiment;

[0040] FIG.5 is a structural block diagram of a transaction processing device in an embodiment;

[0041] FIG.6 is a structural block diagram of a transaction processing device in an embodiment;

[0042] FIG.7 is a structural block diagram of a transaction processing device in an embodiment;

[0043] FIG.8 is an internal structure diagram of a computer device in an embodiment;

[0044] FIG.9 is an internal structure diagram of a computer device in an embodiment.

DETAILED DESCRIPTION

[0045] In order to make the objectives, technical solutions, and advantages of the present disclosure clearer, the present disclosure will be further described in detail below with reference to the accompanying drawings. It should be understood that the specific embodiments described here are only used to explain the application, and not used to limit the application.

[0046] The transaction processing method provided in this application can be applied to the application environment shown in FIG. 1. This application environment involves client 102, endorsing peer 104, ordering peer 106, and committing peer 108. Among them, client 102 communicates with the endorsing peer 104 and the ordering peer 106 respectively through the network. The committing peer 108 communicates with the endorsing peer 104 and the ordering peer 106 respectively through the network. The endorsing peer 104, the ordering peer 106, and the committing peer 108 are located in a blockchain-based Hyperledger Fabric. The client 102 generates a transaction proposal, and sends the transaction proposal to the endorsing peer 104; the endorsing peer 104 simulates the transaction to generate a transaction read-write set, and then sends the transaction read-write set to the client 102 and the committing peer 108; the client 102 sends the transaction information including the transaction proposal and transaction read-write set to the ordering peer 106; the ordering peer 106 sorts and packages the transaction information into blocks, and sends the blocks to the committing peer 108; the committing peer 108 verifies the transaction according to the received transaction read-write set and block. Among them, the client 102 can be, but is not limited to, various personal computers, notebook computers, smart phones, tablet computers, and portable wearable devices. The endorsing peer 104, the ordering peer 106, and the committing peer 108 may be implemented by independent servers or a server cluster composed of multiple servers.

[0047] In some embodiments, as shown in FIG. 2, a transaction processing method is provided. Take the method applied to the client 102 in FIG. 1 as an example for description. Including the following steps S202 to S208.

[0048] S202: The client responds to the transaction request and obtains

identification information and private data corresponding to the transaction request.

[0049] When the transaction is initiated, the client will receive the transaction request. The transaction request can carry identification information and private data. Each transaction corresponds to unique identification information, and private data represents data that is not intended to be disclosed to all peers. When the transaction request carries private data, the transaction request can be regarded as a private transaction request.

[0050] For example, using blockchain to build a commodity trading system, each peer is a supplier, using Hyperledger Fabric as a database to store price information (including purchase prices and selling prices, etc.). However, some suppliers do not want their competitors to know their purchase price, so they will store this price as private data, that is, the data is stored on the chain, but only the supplier and its designated peer have the right to view it, and others on the chain the peer cannot view the data without authorization.

[0051] S204: The client calls the encryption key management contract, generates a key according to the identification information, and uses the generated key to encrypt private data to obtain encrypted private data.

[0052] The encryption key management contract can be pre-deployed in the Hyperledger Fabric system to implement key distribution and management functions. The system management peer can set key generation rules and key authority through the encryption key management contract. For each transaction, a key can be generated as a dedicated key for private data encryption in the transaction, and peers with key authority can obtain the key by calling the encryption key management contract.

[0053] After the client receives the private transaction request and obtains the corresponding identification information and private data, it calls the encryption key management contract. A key is generated according to the identification information, and the generated key is used to encrypt private data to obtain encrypted private data. Since there is a one-to-one correspondence between the transaction and the identification

information, the key generated according to the identification information also has a one-to-one correspondence with the identification information, thereby ensuring that the key corresponding to each transaction is unique and avoiding association between transactions.

[0054] In one embodiment, the identification information includes transaction identification and channel identification. The channel ID indicates the ID of the channel on which the transaction is executed. The client can call the key generation algorithm in the encryption key management contract to generate a key based on the transaction ID and channel ID. For example, if two identifications are spliced into a string of characters according to a specific rule and form as the key, the key can be stored in the encryption key management contract synchronously. Then the client calls the symmetric encryption algorithm in the encryption key management contract. The generated key is used to encrypt the private data to obtain the encrypted private data. In the symmetric encryption algorithm, the encryption key and the decryption key are the same, that is, the encrypted private data can also be decrypted by using the key.

[0055] S206: The client sends a transaction proposal to the endorsing peer, and the transaction proposal includes identification information and encrypted private data; the encryption key management contract is called by the endorsing peer, the corresponding key is obtained according to the identification information, and the obtained key is used to decrypt the encrypted private data, and simulate the transaction to generate the transaction read-write set. Finally, the endorsing peer sends a transaction read-write set to a randomly selected committing peer among the authorized peers that have the right to access private data.

[0056] The client sends a transaction proposal containing identification information and encrypted private data to the endorsing peer. The endorsing peer is specifically a peer among the authorized peers that have the right to access private data. After receiving the transaction proposal, the endorsing peer can call the encryption key management contract, obtain the corresponding key according to the identification information in the transaction proposal, and then use the obtained key to decrypt the encrypted private data

in the transaction proposal. The committing peer is specifically a peer randomly selected from the authorized peers to prevent possible fraud in selecting the same batch of committing peers each time. The endorsing peer sends the transaction read-write set to the committing peer. The committing peer stores the transaction read-write set received from the endorsing peer for subsequent committing.

[0057] S208: The client receives the proposal response returned by the endorsing peer. The proposal response includes the transaction read-write set, which sends transaction information to the ordering peer, and the transaction information includes the transaction read-write set and transaction proposal; The ordering peer generates a block according to the transaction information, and sends the block to the committing peer; the committing peer verifies the validity of the transaction based on the block and the transaction read-write set received from the endorsing peer.

[0058] After the endorsing peer simulates the transaction, it returns the proposal response containing the transaction read-write set to the client. After receiving the proposal response, the client generates transaction information including the transaction read-write set and transaction proposal, and sends the transaction information to the ordering peer. The ordering peer sorts the received transaction information according to time. After sorting is completed, the transaction information is packaged into blocks, and the blocks are sent to the committing peer. The committing peer verifies the validity of the transaction based on the block received from the ordering peer and the transaction read-write set received from the endorsing peer.

[0059] In the above transaction processing method, the encryption key management contract sets the access authority of the private data in the transaction, which can ensure that the private data is only visible to the authorized peers. Use the encryption key management contract to generate a key to encrypt private data, which enables private data to be transmitted in cipher text. At the same time, the private data stored by the authorized peer is not in plaintext form, which can avoid data leakage caused by malicious access and improve the security of private data.

[0060] In one embodiment, before sending the transaction proposal to the endorsing peer, the client also signs the transaction proposal, which can be specifically signed using the client's private key. The client sends the signed transaction proposal to the endorsing peer. After the endorsing peer receives the signed transaction proposal, it first verifies the signed transaction proposal. Specifically, it includes verifying the integrity of the content of the transaction proposal and the legitimacy of the signature, and then proceeding with the endorsement process after the committing is passed.

[0061] In another embodiment, before returning the proposal response to the client, the endorsing peer also signs the proposal response, which can be specifically signed using the private key of the endorsing peer. The endorsing peer returns the signed proposal response to the client. After receiving the signed proposal response, the client first verifies the signed proposal response. Specifically, it includes verifying whether the proposal response meets the legitimacy of the endorsement policy and signature, and sending transaction information to the ordering peer after the committing is passed.

[0062] In one embodiment, as shown in FIG. 3, a transaction processing method is provided. Taking the method applied to the endorsing peer 104 in FIG. 1 as an example for description, the method includes the following steps S302 to S306.

[0063] S302: The endorsing peer gets the transaction proposal sent by the client. The transaction proposal includes identification information and encrypted private data. The encrypted private data is provided by the client in response to the transaction request. Obtain identification information and private data corresponding to the transaction request. Call the encryption key management contract, generate a key based on the identification information, and use the generated key to encrypt private data.

[0064] S304: The endorsing peer calls the encryption key management contract, and obtains the corresponding key according to the identification information. Use the obtained key to decrypt the encrypted private data and simulate the transaction to generate a transaction read-write set. Send a transaction read-write set to a randomly selected committing peer among the authorized peers that have the right to access private

data.

[0065] S306: The endorsing peer returns a proposal response to the client, the proposal response includes the transaction read-write set; the client sends transaction information to the ordering peer, the transaction information includes transaction read-write set and transaction proposal; The ordering peer generates a block according to the transaction information, and sends the block to the committing peer; The committing peer verifies the validity of the transaction based on the block and the transaction read-write set received from the endorsing peer.

[0066] For the specific description of the above steps S302 to S306, reference may be made to the foregoing embodiment, and details are not repeated here. In the above transaction processing method, the encryption key management contract is used to set the access authority of the private data in the transaction to ensure that the private data is only visible to the committing peers. Use the encryption key management contract to generate the key to encrypt the private data, so that the private data is transmitted in cipher text, and the private data stored by the committing peer is not in the form of plaintext, which can avoid data leakage caused by malicious access and improve the security of private data .

[0067] In one embodiment, after the endorsing peer obtains the key, it also uses the obtained key to encrypt the transaction read-write set. Get the encrypted transaction read-write set, and send the encrypted transaction read-write set to all authorized peers. The authorized peers store the encrypted transaction read-write set locally.

[0068] Specifically, the endorsing peer may use the obtained key to encrypt the transaction read-write set through a symmetric encryption algorithm. In the symmetric encryption algorithm, the encryption key and the decryption key are the same, that is, the encryption key can also be used to decrypt the encrypted transaction read-write set. Authorized peers can store the encrypted transaction read-write set in a local private database. Since the data is stored in cipher text, the risk of data leakage can be reduced. In addition, the authorized peer has the authority to obtain the key, and can use the key to

decrypt and restore the locally stored encrypted data when necessary, which facilitates the search and comparison of private data.

[0069] In one embodiment, before sending the transaction proposal to the endorsing peer, the client also signs the transaction proposal, which can be specifically signed using the client's private key. The client sends the signed transaction proposal to the endorsing peer. After obtaining the signed transaction proposal, the endorsing peer first verifies the signed transaction proposal. Specifically, it includes verifying the integrity of the transaction proposal content and the legality of the signature. After the committing is passed, the endorsement process is carried out.

[0070] In another embodiment, before returning the proposal response to the client, the endorsing peer also signs the proposal response, which can be signed using the private key of the endorsing peer. The endorsing peer returns the signed proposal response to the client. After receiving the signed proposal response, the client first verifies the signed proposal response. Specifically, it includes verifying whether the proposal response meets the legitimacy of the endorsement policy and signature, and sending transaction information to the ordering peer after the committing is passed.

[0071] In one embodiment, as shown in FIG. 4, a transaction processing method is provided. Taking the method applied to the committing peer 108 in FIG. 1 as an example for description, the method includes the following steps S402 to S406.

[0072] S402: The committing peer receives the transaction read-write set sent by the endorsing peer; In the transaction read-write set, the endorsing peer obtains the transaction proposal including identification information and encrypted private data sent by the client. The transaction read-write set is generated by the endorsing peer. First, the endorsing peer obtains the transaction proposal including identification information and encrypted private data sent by the client. Second, call the encryption key management contract to obtain the corresponding key according to the identification information. Third, use the obtained key to decrypt the encrypted private data. Fourth, simulate the transaction to generate a read-write set; the encrypted private data is responded to the

transaction request by the client. The encrypted private data is obtained in three steps. First, in response to the transaction request, the client obtains the identification information and private data corresponding to the transaction request. Second, call the encryption key management contract to generate a key based on the identification information, and finally, the generated key encrypts private data.

[0073] S404: The committing peer gets the block sent by the ordering peer; the block is generated by the ordering peer based on the transaction information received from the client. The transaction information includes the transaction proposal and the transaction read-write set in the proposal response returned by the endorsing peer.

[0074] S406: The committing peer verifies the validity of the transaction according to the block and the transaction read-write set received from the endorsing peer.

[0075] For the specific description of the foregoing steps S402 to S406, reference may be made to the foregoing embodiment, which is not repeated here. In the above transaction processing method, the encryption key management contract is used to set the access authority of the private data in the transaction to ensure that the private data is only visible to the authorized peers. Use the encryption key management contract to generate the key to encrypt the private data so that the private data is transmitted in cipher text. At the same time, the private data stored by the authorized peers is not in plaintext form, which can avoid data leakage caused by malicious access and improve the security of private data.

[0076] In one embodiment, after obtaining the key, the endorsing peer also uses the obtained key to encrypt the transaction read-write set to obtain the encrypted transaction read-write set. The endorsing peer sends the encrypted transaction read-write set to the committing peer, and the committing peer receives the encrypted transaction read-write set sent by the endorsing peer, and locally stores the encrypted transaction read-write set.

[0077] Specifically, the endorsing peer may use the obtained key to encrypt the transaction read-write set through a symmetric encryption algorithm. In the symmetric encryption algorithm, the encryption key and the decryption key are the same, that is, the

encryption key can also be used to decrypt the encrypted transaction read-write set. The committing peer can store the encrypted transaction read-write set to a local private database. Since the data is stored in cipher text form, the risk of data leakage can be reduced. In addition, the committing peer has the authority to obtain the key, and can use the key to decrypt and restore the locally stored encrypted data when necessary, which facilitates the search and comparison of private data.

[0078] In one embodiment, the committing peer reads-writes the set according to the block and the transaction received from the endorsing peer. Before verifying the validity of the transaction, the transaction read-write set received from the endorsing peer is also verified. Specifically, the committing peer respectively performs hash calculation on the transaction read-write set in the block and the transaction read-write set received from the endorsing peer to obtain the first hash value and the second hash value. By comparing the first hash value with the second hash value, the transaction read-write set received from the endorsing peer is verified. If the first hash value is consistent with the second hash value, it means that the data has not been lost or tampered with. According to the transaction read-write set received from the endorsing peer, a simulated transaction is performed to determine whether there is a conflicting transaction. If there is no conflicting transaction, the transaction is valid. If the transaction is valid, the data on the chain is changed and the new data is written into the block at the same time. If the transaction is invalid, the data on the chain is not changed.

[0079] In one embodiment, a transaction processing method is provided. The method is applied to the interaction among the client 102, the endorsing peer 104, the ordering peer 106, and the committing peer 108 in FIG. 1 as an example for description, including the following steps :

[0080] In response to the transaction request, the client terminal obtains identification information and private data corresponding to the transaction request. The identification information includes transaction identification and channel identification.

[0081] The client calls the key generation algorithm in the encryption key

management contract. Generate a key based on the transaction ID and channel ID, and call the symmetric encryption algorithm in the encryption key management contract. Use the generated key to encrypt the private data, obtain the encrypted private data, and store the generated key in the encryption key management contract.

[0082] The client generates a transaction proposal and signs the transaction proposal. The client sends a signed transaction proposal to the endorsing peer. The transaction proposal includes identification information and encrypted private data.

[0083] The endorsing peer verifies the signed transaction proposal. After the committing is passed, the encryption key management contract is called. Obtain the corresponding key according to the identification information, and use the obtained key to decrypt the encrypted private data. The simulated transaction generates a transaction read-write set, and sends the transaction read-write set to a randomly selected committing peer among the authorized peers that have access to private data.

[0084] The endorsing peer uses the obtained key to encrypt the transaction read-write set, and obtains the encrypted transaction read-write set. The encrypted transaction read-write set is sent to all authorized peers, and the authorized peer stores the encrypted transaction read-write set locally.

[0085] The endorsing peer generates a proposal response, signs the proposal response, and sends the signed proposal response to the client. The proposal response includes the transaction read-write set.

[0086] The client commits the signed proposal response. After the commission is passed, the transaction information is sent to the ordering peer. Transaction information includes transaction read-write set and transaction proposal.

[0087] The ordering peer sorts the transaction information according to time. The sorted transaction information is packaged into blocks, and the blocks are sent to the committing peer.

[0088] The committing peer compares the hash value of read-write set received

from transactions in the block and the hash value of the set received from the endorsing peer, after the committing is passed, the committing peer commits the validity of the transaction based on the transaction read-write set received from the endorsing peer.

[0089] For the specific description of the foregoing steps S402 to S406, reference may be made to the foregoing embodiment, which is not repeated here. In the above transaction processing method, the encryption key management contract is used to set the access authority of the private data in the transaction to ensure that the private data is only visible to the authorized peers, and the encryption key management contract is used to generate the key to encrypt the private data so that the private data is in cipher text. The way that data transmits in the form of cipher text can also improve the security of private data. The authorized peers store the encrypted transaction read-write set locally. Since the data is stored in ciphertext form, the risk of data leakage can be reduced. In addition, the authorized peer has the authority to obtain the key, and can use the key to decrypt and restore the locally stored encrypted data when necessary (for example, when data is found to be lost or inconsistent), which facilitates the search and comparison of private data.

[0090] It should be understood that, although the steps in the flowcharts involved in the foregoing embodiments are displayed in sequence as indicated by the arrows, these steps are not necessarily executed in sequence in the order indicated by the arrows. Unless specifically stated in this article, the execution of these steps is not strictly limited in order, and these steps can be executed in other orders. Moreover, at least part of the steps in the flowcharts involved in the above-mentioned embodiments may include multiple steps or multiple stages. These steps or stages are not necessarily executed at the same time, but may be executed at different times. Or the execution order of the stages is not necessarily carried out sequentially, but may be executed alternately or alternately with other steps or at least part of the steps or stages in other steps.

[0091] In one embodiment shown in FIG. 5, a transaction processing device 500 is provided. The device is applied to the client and includes: an acquisition module 510, an encryption module 520, a sending module 530, and a receiving module 540, wherein:

[0092] The obtaining module 510 is configured to obtain identification information and private data corresponding to the transaction request, then the module responds to the request.

[0093] The encryption module 520 is used to call the encryption key management contract, generate a key according to the identification information, and use the generated key to encrypt private data to obtain encrypted private data.

[0094] The sending module 530 is used to send a transaction proposal request to the endorsing peer. The transaction proposal includes identification information and encrypted private data; the endorsing peer calls the encryption key management contract, and the peer obtains the corresponding key according to the identification information, and uses the obtained key to decrypt the encrypted private data, then the peer generates the transaction read-write set by simulating the transaction, and the transaction read-write set is sent to the committing peer which is randomly selected among the authorized peers with the right to access the private data.

[0095] The receiving module 540 is configured to receive the proposal response returned by the endorsing peer, and the proposal response includes a transaction read-write set.

[0096] The sending module 530 is also used to send transaction information to the ordering peer. The transaction information includes the transaction read-write set and transaction proposal; the ordering peer generates a block based on the transaction information and sends the block to the committing peer; the committing peer commits the validity of the transaction according to the block information and the transaction read-write set received from endorsing peer.

[0097] In one embodiment, the identification information includes a transaction identification and a channel identification; the encryption module 520 is specifically configured to call the key generation algorithm in the encryption key management contract, and generate a key based on the transaction identification and the channel identification, then call the symmetric encryption algorithm in the encryption key

management contract. The encryption algorithm uses the generated key to encrypt private data to obtain encrypted private data.

[0098] In one embodiment, the sending module 530 is also used to sign the transaction proposal, and send the signed transaction proposal to the endorsing peer; the endorsing peer verifies the signed transaction proposal before calling the encryption key management contract.

[0099] In one embodiment, the receiving module 540 is also used to receive the signed proposal response returned by the endorsing peer; the sending module 530 is also used to verify the signed proposal response before sending the transaction information to the ordering peer.

[00100] In one embodiment shown in FIG. 6, a transaction processing device 600 is provided, which is applied to the endorsing peer, and includes: an acquisition module 610, a processing module 620, and a return module 630, wherein:

[00101] The obtaining module 610 is used to obtain the transaction proposal sent by the client. The transaction proposal includes identification information and encrypted private data. The client responds to the transaction request to obtain the identification information and private data corresponding to the transaction request. The encryption key management contract generates a key according to the identification information, and uses the generated key to encrypt private data, finally it generates the encrypted private data.

[00102] The processing module 620 is used to call the encryption key management contract, obtain the corresponding key according to the identification information, and use the obtained key to decrypt the encrypted private data, simulate the transaction to generate the transaction read-write set, and send it to the committing peers which are randomly selected from the authorized peers(the authorized peers have the right to access the private data).

[00103] The return module 630 is used to return a proposal response to the client. The proposal response includes the transaction read-write set; the client sends transaction

information which includes the transaction read-write set and transaction proposal to the ordering peer; the ordering peer generates a block based on the transaction information, then sends the block to the committing peer; the committing peer commits the validity of the transaction according to the block and the transaction read-write set received from the endorsing peer.

[00104] In one embodiment, the processing module 620 is further configured to use the obtained key to encrypt the transaction read-write set to obtain the encrypted transaction read-write set; send the encrypted transaction read-write set to all authorized peers, and the authorized peers store the transaction read-write set locally.

[00105] In one embodiment, the obtaining module 610 is also used to obtain the signed transaction proposal sent by the client; the processing module 620 is also used to commit the signed transaction proposal before calling the encryption key management contract.

[00106] In one embodiment, the return module 630 is also used to sign the proposal response and return the signed proposal response to the client; the client verifies the signed proposal response before sending the transaction information to the ordering peer.

[00107] In one embodiment shown in FIG. 7, a transaction processing device 700 is provided, which is applied to the committing peer and includes: a receiving module 710, an obtaining module 720, and a committing module 730, wherein:

[00108] The receiving module 710 is used to receive the transaction read-write set sent by the endorsing peer; the endorsing peer obtains the transaction proposal including identification information and encrypted private data sent by the client, then calls the encryption key management contract, obtains the corresponding key according to the identification information, finally uses the obtained key to decrypt the encrypted private data to simulate the transaction and obtains the transaction read-write set; the client responds to the transaction request to obtain the identification information and private data corresponding to the transaction request, calls the encryption key management contract and generates a key, the generated key is used to encrypt private data, finally it

generates the encrypted private data.

[00109] The obtaining module 720 is used to obtain the block sent by the ordering peer; the block is generated by the ordering peer according to the transaction information received from the client, the transaction information includes the transaction proposal and the transaction read-write set in the proposal response returned by the endorsing peer;

[00110] The committing module 730 is used to commit the validity of the transaction according to the block and the transaction read-write set received from the endorsing peer.

[00111] In one embodiment, the receiving module 710 is also used to receive the encrypted transaction read-write set sent by the endorsing peer. The encrypted transaction read-write set is obtained by encrypting the transaction read-write set with the key obtained by the endorsing peer; and the encrypted transaction read-write sets are stored locally.

[00112] In one embodiment, before committing the validity of the transaction, module 730 is also used to make hash calculation of both read-write set received from transactions in the block and set received from the endorsing peer. The transaction read-write set received from block is hashed to obtain the first hash value, and the transaction read-write set received from endorsing peer is hashed to obtain the second hash value; by comparing the first hash value with the second hash value, the transaction read-write set received from the endorsing peer is committed.

[00113] For the specific limitation of the transaction processing device, please refer to the above limitation of the transaction processing method, which will not be repeated here. Each module in the above transaction processing device can be implemented in whole or in part by software, hardware, and combinations thereof. The foregoing modules may be embedded in the form of hardware or independent of the processor in the computer device, or may be stored in the memory of the computer device in the form of software, so that the processor can call and execute the operations corresponding to

the foregoing modules.

[00114] In one embodiment, a computer device is provided. The computer device may be a server, and its internal structure diagram can be as shown in FIG. 8. The computer equipment includes a processor, a memory, and a network interface connected through a system bus. Among them, the processor of the computer device is used to provide calculation and control capabilities. The memory of the computer device includes a non-volatile storage medium and an internal memory. The non-volatile storage medium stores an operating system, a computer program, and a database. The internal memory provides an environment for the operation of the operating system and computer programs in the non-volatile storage medium. The network interface of the computer device is used to communicate with an external terminal through a network connection. The computer program is executed by the processor to realize a transaction processing method.

[00115] In one embodiment, a computer device is provided. The computer device may be a terminal, and its internal structure diagram can be as shown in FIG. 9. The computer equipment includes a processor, a memory, a communication interface, a display screen and an input device connected through a system bus. Among them, the processor of the computer device is used to provide calculation and control capabilities. The memory of the computer device includes a non-volatile storage medium and an internal memory. The non-volatile storage medium stores an operating system and a computer program. The internal memory provides an environment for the operation of the operating system and computer programs in the non-volatile storage medium. The communication interface of the computer device is used for wired or wireless communication with an external terminal. The wireless method can be implemented through WIFI, operator network, NFC (near field communication) or other technologies. The computer program is executed by the processor to realize a transaction processing method. The display screen of the computer equipment can be a liquid crystal display screen or an electronic ink display screen, and the input device of the computer equipment can be a touch layer covered on the display screen, or it can be a button, a

trackball or a touchpad set on the housing of the computer equipment. It can also be an external keyboard, touchpad, or mouse.

[00116] Those skilled in the art can understand that the structure shown in FIG. 8 or FIG. 9 is only a block diagram of part of the structure related to the solution of the present application, and does not constitute a limitation on the computer equipment to which the solution of the present application is applied. The computer device may include more or fewer components than shown in the figures, or combine certain components, or have a different component arrangement.

[00117] In one embodiment, a computer device is provided, including a memory and a processor, and a computer program is stored in the memory, and the processor implements the steps in the foregoing method embodiments when executing the computer program.

[00118] In one embodiment, a computer-readable storage medium is provided, on which a computer program is stored, and the computer program is executed by a processor to implement the steps in the foregoing method embodiments.

[00119] In one embodiment, a computer program product or computer program is provided. The computer program product or computer program includes computer instructions, and the computer instructions are stored in a computer-readable storage medium. The processor of the computer device reads the computer instruction from the computer-readable storage medium, and the processor executes the computer instruction, so that the computer device executes the steps in the foregoing method embodiments.

[00120] It should be understood that the terms "first", "second", etc. in the foregoing embodiments are only used for descriptive purposes, and cannot be understood as indicating or implying relative importance or implicitly indicating the number of indicated technical features.

[00121] A person of ordinary skill in the art can understand that all or part of the processes in the above-mentioned embodiment methods can be implemented by instructing relevant hardware through a computer program. The computer program can

be stored in a non-volatile computer readable storage. In the medium, when the computer program is executed, it may include the procedures of the above-mentioned method embodiments. Wherein, any reference to memory, storage, database or other media used in the embodiments provided in this application may include at least one of non-volatile and volatile memory. Non-volatile memory may include read-only memory (Read-Only Memory, ROM), magnetic tape, floppy disk, flash memory, or optical memory. Volatile memory may include random access memory (Random Access Memory, RAM) or external cache memory. As an illustration and not a limitation, the RAM may be in various forms, such as static random access memory (Static Random Access Memory, SRAM) or dynamic random access memory (Dynamic Random Access Memory, DRAM).

[00122] The technical features of the above embodiments can be combined arbitrarily. In order to make the description concise, all possible combinations of the technical features in the above embodiments are not described. However, as long as there is no contradiction between the combinations of these technical features, they should be considered as the range described in this specification.

[00123] The above-mentioned embodiments only express several implementation manners of the present application, and the description is relatively specific and detailed, but it should not be understood as a limitation on the scope of the invention patent. It should be pointed out that for those of ordinary skill in the art, without departing from the concept of this application, several modifications and improvements can be made, and these all fall within the protection scope of this application. Therefore, the scope of protection of the patent of this application shall be subject to the appended claims.

CLAIMS

What is claimed is:

1. A transaction processing method, characterized in that the method is applied to the client, and includes:

The client responds to the transaction request and obtains identification information and private data corresponding to the transaction request;

The client calls the encryption key management contract, generates a key according to the identification information, and uses the generated key to encrypt private data to obtain encrypted private data;

The client sends a transaction proposal to the endorsing peer, and the transaction proposal includes identification information and encrypted private data; the encryption key management contract is called by the endorsing peer, the corresponding key is obtained according to the identification information, and the obtained key is used to decrypt the encrypted private data, and simulate the transaction to generate the transaction read-write set. Finally, the endorsing peer sends a transaction read-write set to a randomly selected committing peer among the authorized peers that have the right to access private data;

The client receives the proposal response returned by the endorsing peer. The proposal response includes the transaction read-write set, which sends transaction information to the ordering peer, and the transaction information includes the transaction read-write set and transaction proposal; The ordering peer generates a block according to the transaction information, and sends the block to the committing peer; the committing peer verifies the validity of the transaction based on the block and the transaction read-write set received from the endorsing peer.

2. The method according to claim 1, wherein the identification information includes a transaction identification and a channel identification; calling the encryption key management contract, generating a key based on the identification information, and using the generated key encrypting the private data to obtain encrypted private data includes:

The client calls the key generation algorithm in the encryption key management contract, and generate a key according to the transaction identifier and the channel identifier;

The symmetric encryption algorithm in the encryption key management contract is called, and the private data is encrypted with the generated key to obtain encrypted private data.

3. The method according to claim 1, wherein before sending the transaction proposal to the endorsing peer, the method further comprises: signing the transaction proposal;

Sending a transaction proposal to the endorsing peer includes: sending a signed transaction proposal to the endorsing peer; the endorsing peer verifies the signed transaction proposal before calling the encryption key management contract.

4. The method according to claim 3, wherein receiving the proposal response returned by the endorsing peer comprises: receiving the signed proposal response returned by the endorsing peer;

Before sending the transaction information to the ordering peer, it further includes: verifying the signed proposal response.

5. A transaction processing method, characterized in that the method is applied to

endorsing peer, and includes:

The endorsing peer obtains a transaction proposal sent by the client, the transaction proposal includes identification information and encrypted private data, and the client responds to the transaction request to obtain the identification information and private data corresponding to the transaction request; calls an encryption key management contract, generates a key according to the identification information, and encrypts the private data with the generated key;

The endorsing peer calls the encryption key management contract, obtains the corresponding key according to the identification information, and uses the obtained key to decrypt the encrypted private data, simulates a transaction to generate a transaction read-write set, and sends the transaction read-write set to the committing peer randomly selected among the authorized peers that have access to the private data;

A proposal response is returned to the client, the proposal response includes the transaction read-write set; the client sends the transaction information to the ordering peer, the transaction information includes the transaction read-write set and the transaction proposal; the ordering peer generates a block based on the transaction information, and sends the block to the committing peer; the committing peer based on the block and the transaction read and write set received from the endorsing peer to verify the validity of the transaction.

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

The endorsing peer encrypts the transaction read-write set with the obtained key, and obtains the encrypted transaction read-write set;

The endorsing peer sends the encrypted transaction read-write set to all authorized peers, and the authorized peer stores the encrypted transaction read-write set locally.

7. The method according to claim 5, wherein obtaining a transaction proposal sent by the client includes: obtaining a signed transaction proposal sent by the client;

Before calling the encryption key management contract, the endorsing peer also includes: verifying the signed transaction proposal.

8. The method according to claim 7, wherein before returning the proposal response to the client, the method further comprises: signing the proposal response;

The endorsing peer returns a proposal response to the client that includes: returning a signed proposal response to the client; the client verifies the signed proposal response before sending transaction information to the ordering peer.

9. A transaction processing device, characterized in that the device is applied to the client and includes:

An acquisition module is used to obtain identification information and private data corresponding to the transaction request in response to the transaction request;

An encryption module is used to call an encryption key management contract, generate a key according to the identification information, and use the generated key to encrypt the private data to obtain encrypted private data;

A sending module is used to send a transaction proposal to the endorsing peer, the transaction proposal includes the identification information and the encrypted private data; the endorsing peer calls the encryption key management contract, and obtains the corresponding key, and uses the obtained key to decrypt the encrypted private data,

simulates a transaction to generate a transaction read-write set, and sends the transaction read-write set to the committing peer randomly selected among the authorized peers that have access to the private data;

A receiving module, configured to receive a proposal response returned by the endorsing peer, where the proposal response includes the transaction read-write set;

A sending module is also used to send transaction information to the ordering peer, the transaction information includes the transaction read-write set and the transaction proposal; the ordering peer generates a block according to the transaction information, and sends it to the committing peer; the committing peer verifies the validity of the transaction based on the block and the transaction read-write set received from the endorsing peer.

10. A computer device comprising a memory and a processor, the memory storing a computer program, wherein the processor executes the computer program to implement the method according to any one of claims 1 to 9 step.

11. A computer-readable storage medium having a computer program stored thereon, wherein the computer program implements the steps of the method according to any one of claims 1 to 9 when the computer program is executed by a processor.

ABSTRACT

This application relates to a transaction processing method, device, computer equipment and storage medium. The method includes: responding to a transaction request, obtaining corresponding identification information and private data; calling an encryption key management contract to generate a key based on the identification information, and encrypting the private data with the key; sending the identification information and encrypted private data to the endorsing peer transaction proposal; The encryption key management contract is called by the endorsing peer to obtain the key according to the identification information, and use the key to decrypt the encrypted private data. Simulate transaction to generate transaction read-write set, and send transaction read-write set to randomly selected committing peers among authorized peers that have access to private data. Receive the proposal response including the transaction read-write set returned by the endorsing peer, and send the transaction information including the transaction read-write set and transaction proposal to the ordering peer. The ordering peer generates a block according to the transaction information, and sends the block to the committing peer; the committing peer verifies the validity of the transaction. Using this method can improve the security of private data.

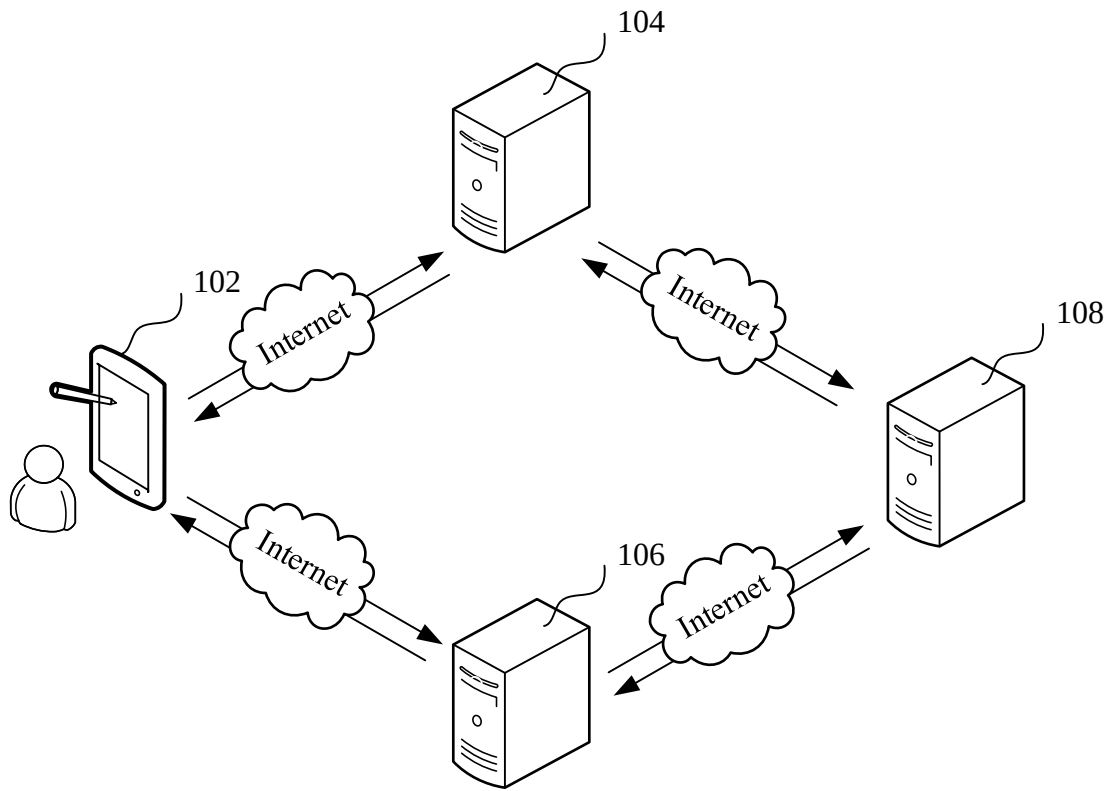


FIG. 1

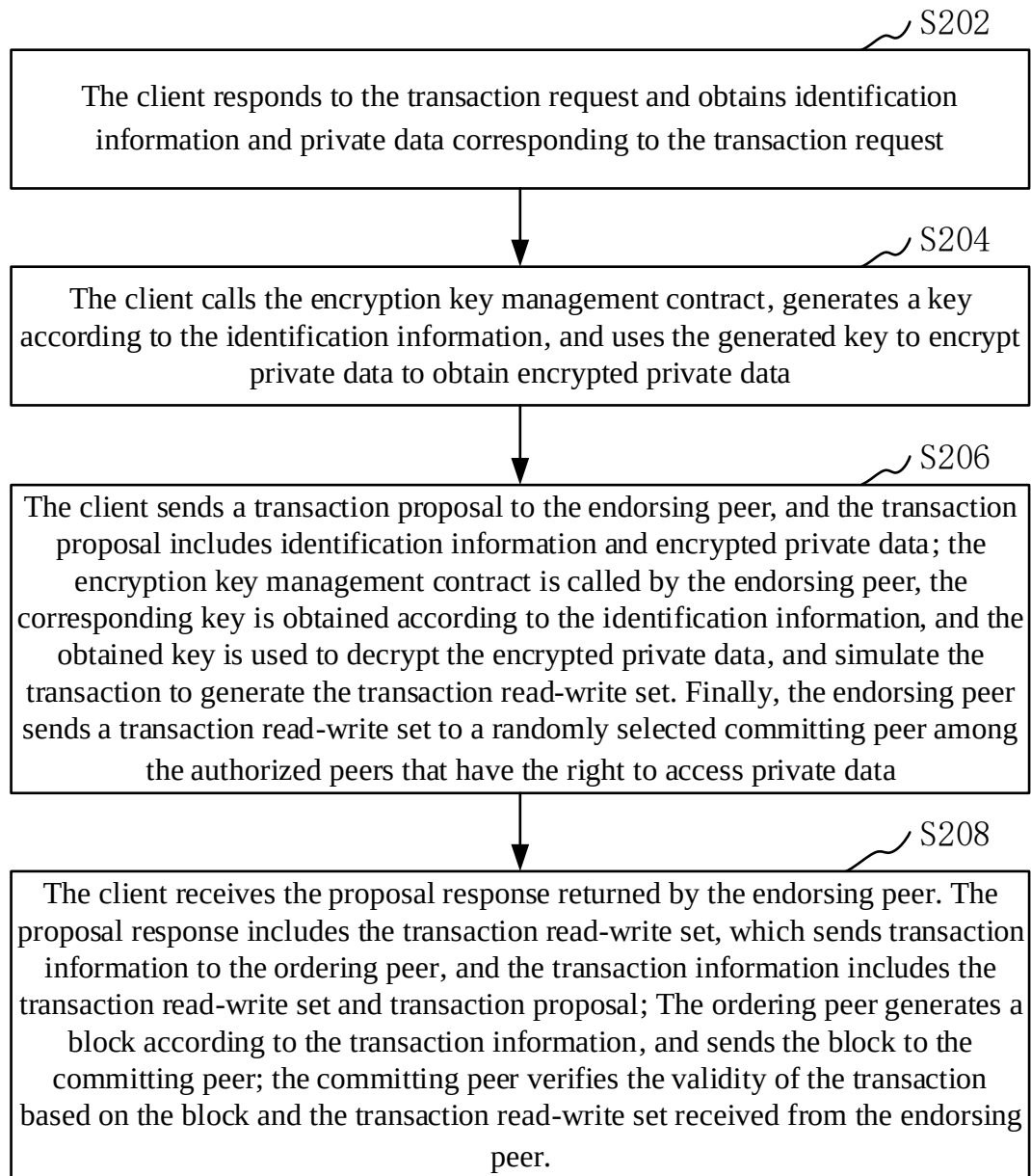


FIG. 2

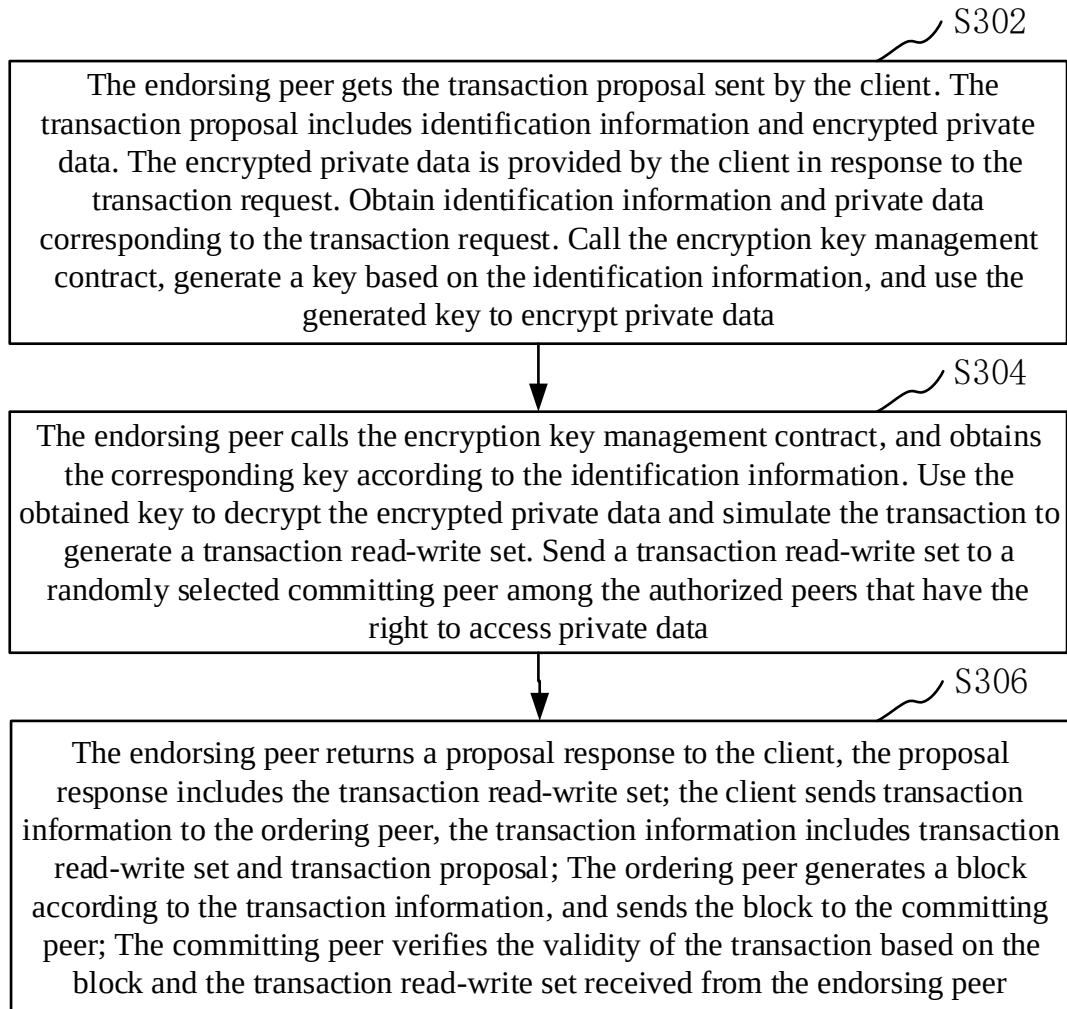


FIG. 3

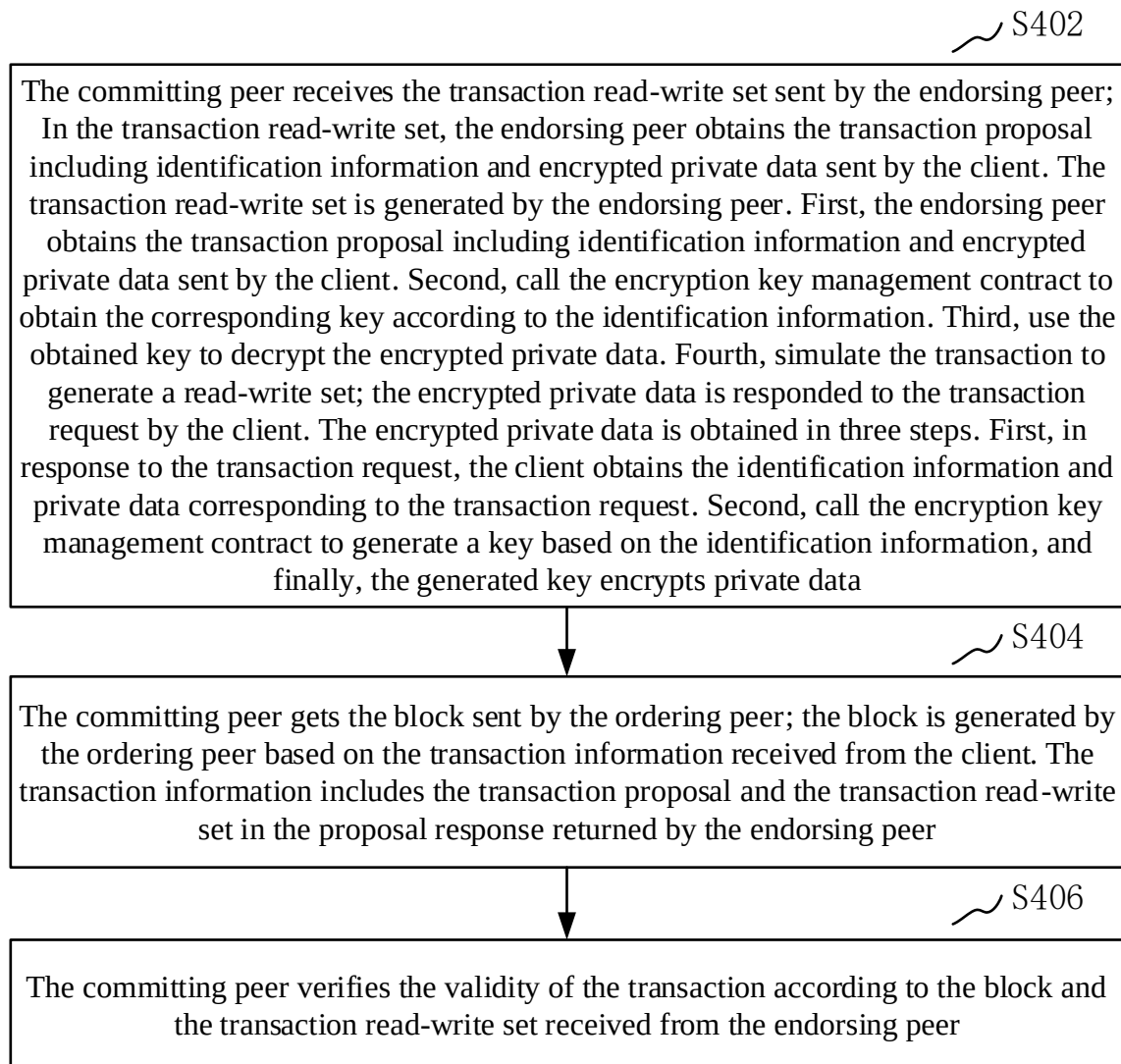


FIG. 4

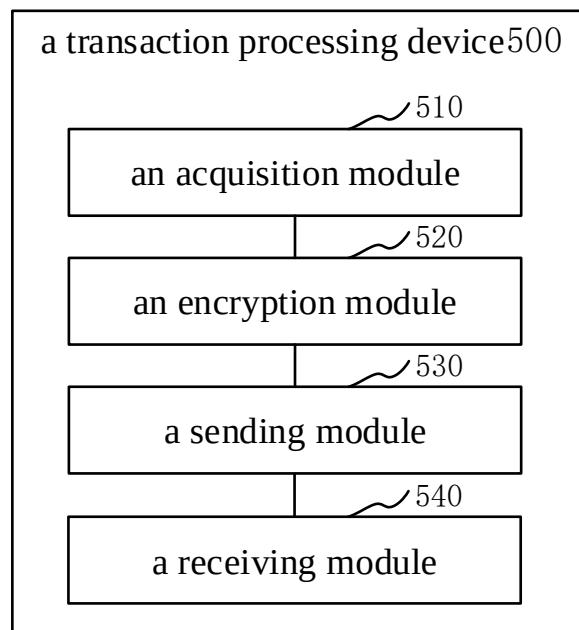


FIG. 5

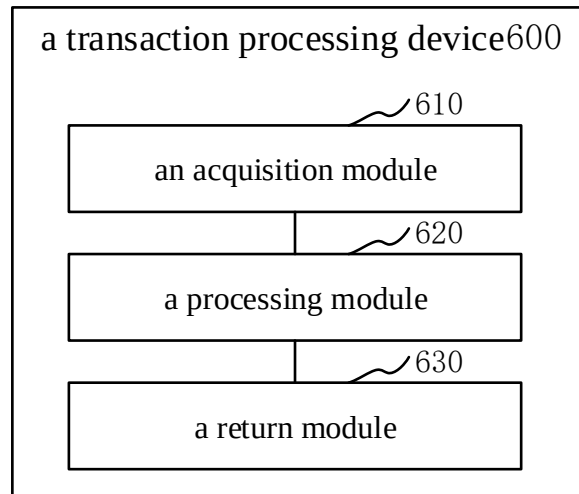


FIG. 6

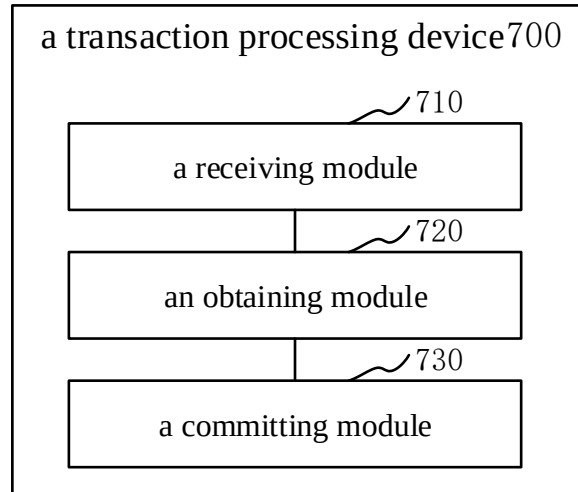


FIG. 7

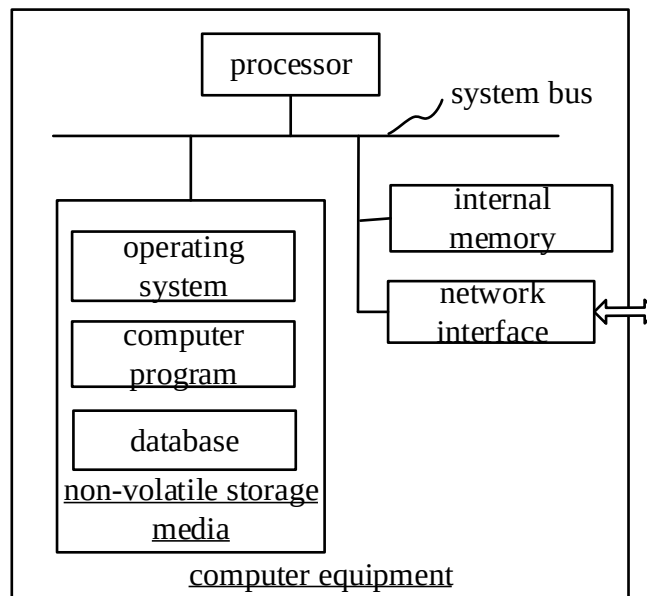


FIG. 8

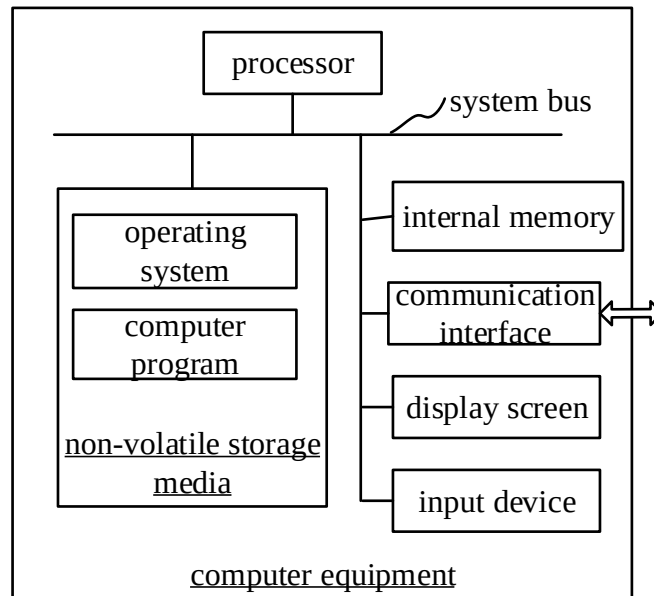


FIG. 9