DATA SYNCHRONIZATION METHOD AND APPARATUS, COMPUTER DEVICE AND READABLE STORAGE MEDIUM

RELATED APPLICATION

[0001] This application claims priority to Chinese Patent Application No. 201910196407.9, entitled "METHOD AND APPARATUS FOR DATA SYCHRONIZATION, COMPUTER DEVICE, AND READABLE STORAGE MEDIUM" filed with the China National Intellectual Property Administration on March 15, 2019, which is incorporated herein by reference in its entirety.

FIELD OF THE TECHNOLOGY

[0002] This application relates to the field of blockchain technology, and in particular, to a method and an apparatus for data synchronization, a computer device, and a readable storage medium.

BACKGROUND OF THE DISCLOSURE

[0003] With the development of network technology, people may search networks for data through a browser to obtain information. Some data may carry a sensitive phrase, and in such case, a device with an installed browser would screen the sensitive phrase in the to-be-queried data when displaying the to-be-queried data to a user. The to-be-queried data is displayed to the user after being filtered, so as to prevent a wide spread of the sensitive phrase.

[0004] At present, the device with the installed browser may seek help from a sensitive phrase filtering system, for screening the sensitive phrase in the to-be-queried data. Each time the to-be-queried data is to be filtered, the device needs to activate the sensitive phrase filtering system to implement the filtering, and then wait for a filtering result fed back by the sensitive phrase filtering system. That results in a long waiting time and a low efficiency when the device screens the sensitive phrase. Therefore, there is an urgent need for a method for synchronizing a database of sensitive phrases.

SUMMARY

[0005] A method and an apparatus for data synchronization, a computer device, and a readable storage medium are provided according to various embodiments of the present disclosure.

[0006] A method for data synchronization is provided. The method is performed on a computer device, and includes:

receiving a piece of transaction data, where the piece of transaction data carries an update-operation identifier and a sensitive phrase corresponding to the update-operation identifier;

obtaining the update-operation identifier and the sensitive phrase from a target block including the piece of transaction data, in a case that the target block is stored into a blockchain of a blockchain system; and

updating a database of sensitive phrases according to the update-operation identifier and the sensitive phrase from the target block.

[0007] A apparatus for data synchronization is provided, including:

a receiving module, configured to receive a piece of transaction data, where the piece of transaction data carries an update-operation identifier and a sensitive phrase corresponding to the update-operation identifier;

an obtaining module, configured to obtain the update-operation identifier and the sensitive phrase from a target block including the piece of transaction data, in a case that the target block is stored into a blockchain of a blockchain system; and

an update module, configured to update a database of sensitive phrases according to the update-operation identifier and the sensitive phrase from the target block.

[0008] A non-volatile storage medium is provided, storing computer-readable instructions. The computer-readable instructions when executed by one or more processors configure the one or more processors to perform the steps of the method for data synchronization.

[0009] A computer device is provided, including a memory and a processor. The memory stores computer-readable instructions, and the computer-readable instructions when executed by the processor configure the processor to perform the steps of the method for data synchronization.

[0010] Hereinafter details are provided in drawings and description for one or more embodiments of the present disclosure. Other features, objectives, and advantages of the present disclosure are apparent from specification, drawings, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] For clearer illustration of the technical solutions according to embodiments of the present disclosure, hereinafter briefly described are the drawings to be applied in embodiments of the

present disclosure or conventional techniques. Apparently, the drawings in the following descriptions are only some embodiments of the present disclosure, and other drawings may be obtained by those skilled in the art based on the provided drawings without creative efforts.

[0012] Figure 1 is a schematic diagram of a blockchain system according to an embodiment of the present disclosure;

[0013] Figure 2 is a flowchart of a method for data synchronization according to an embodiment of the present disclosure;

[0014] Figure 3 is a flowchart of a method for data query based on data synchronization according to an embodiment of the present disclosure;

[0015] Figure 4 is a schematic structural diagram of an apparatus for data synchronization according to an embodiment of the present disclosure; and

[0016] Figure 5 is a schematic structural diagram of a node device according to an embodiment of the present disclosure.

DESCRIPTION OF EMBODIMENTS

[0017] To make the object, technical solutions and advantages of the present application clearer, hereinafter the present application will be further described in conjunction with the drawings in the embodiments of the present application. It is appreciated that embodiments described herein are merely intended to explain the present disclosure instead of limiting the present disclosure.

[0018] Figure 1 is a schematic diagram of a blockchain system according to an embodiment of the present disclosure. Reference is made to Figure 1, in which the blockchain system includes at least two node devices. The at least two node devices may belong to different users. Any node device may generate or receive transaction data, package at least one piece of transaction data, generate a block, and store a block on which a consensus is reached. The transaction data may be data of any type, and may include any content. Any data received or generated by any node device in the blockchain system may be referred to as transaction data.

[0019] Node devices in the blockchain system may have different functions in the blockchain system, and the node device may be categorized as a supervisory node device or a common node device. The supervisory node device may serve as a supervisor configured to publish transaction data carrying a sensitive phrase in the blockchain system, so that another node

device may update a local database of sensitive phrases according to the sensitive phrase published by the supervisory node device.

[0020] Any node device may provide a query service for a user, so that the user may use such node device to search each block in a blockchain of the blockchain system for transaction data. When a node device displays transaction data in a to-be-searched block to the user, the node device may screen a sensitive phrase in the transaction data in the to-be-searched block according to sensitive phrases in a local database, and then display the filtered transaction data to the user.

[0021] Hereinabove described is the blockchain system and the node devices. Reference is made to Figure 2, which illustrates a process of a node device in a blockchain system storing a sensitive phrase published by a supervisory node device into a local database of sensitive phrases. Figure 2 is a flowchart of a method for data synchronization according to an embodiment of the present disclosure. The method includes following steps 201 to 207.

[0022] In step 201, a supervisory node device generates a piece of transaction data. The piece of transaction data carries an update-operation identifier and a sensitive phrase corresponding to the update-operation identifier.

[0023] The supervisory node device may be any node device provided with supervisory authority in the blockchain system. The update-operation identifier may be configured to indicate an update operation that a node device needs to perform. The update-operation identifier may be an addition identifier or may be a deletion identifier. The addition identifier is configured to indicate adding a sensitive phrase to the database of sensitive phrases. The deletion identifier is configured to indicate deleting a sensitive phrase from the database of sensitive phrases.

[0024] In one embodiment, the update-operation identifier may be a character string, or may be implemented in another form. Different character strings for the update-operation identifier may represent different update operations. For example, "Add" represents an adding operation, and "Delete" represents a deleting operation.

[0025] Each node device in the blockchain system is provided with the database of sensitive phrases. The database of sensitive phrases is configured to store a sensitive phrase. The sensitive phrase may be any phrase, and content of the sensitive phrase is not limited in embodiments of the present disclosure.

[0026] The supervisory node device performs the step 201 when receiving a request for generating transaction data. The request for generating transaction data is configured to request generating a piece of transaction data carrying a sensitive phrase. In one embodiment, the

supervisory node device receives a request for generating transaction data, and the request for generating transaction data includes the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier. The supervisory node device generates a piece of transaction data that meets a format requirement on transaction data in the blockchain system, based on the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier that are in the request for generating transaction data.

[0027] The supervisory node device receiving the request for generating transaction data may be triggered by a storage operation of the user. For example, the user selects an update option in a user interface of the supervisory node device, enters a sensitive phrase at a phrase position corresponding to the update option, and then clicks a storage option, and the request for generating transaction data may be triggered accordingly.

[0028] The piece of transaction data may further include a supervision identifier configured to indicate that the piece of transaction data is generated by the supervisory node device. The supervision identifier includes a signature of the supervisory node device or an address of the supervisory node device. The signature of the supervisory node device may be written on the piece of transaction data by the supervisory node device using a private key. The address of the supervisory node device may be an Internet protocol (IP) address of the supervisory node device, or may be another address capable of identifying the supervisory node device. The supervision identifier is not specifically limited herein.

[0029] In one embodiment, the supervisory node device adds the address thereof to an initiator-address field of the piece of transaction data. The supervisory node device adds the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier to a comment field of the piece of transaction data.

[0030] In one embodiment, the supervisory node device adds the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier to a comment field of the piece of transaction data. The supervisory node device signs the commented piece of transaction data by using the private key of the supervisory node device.

[0031] The supervisory node device may arrange the update-operation identifier and the sensitive phrase in a same row when adding them to the comment field of target transaction data, so as to show that the update-operation identifier corresponds to the sensitive phrase. For example, "Add" serves as the addition identifier, "Delete" serves as the deletion identifier, and the comment is in a form of a table. Reference is made to Table 1, in which sensitive phrases 1 to n in the first

row all correspond to the addition identifier "Add", and sensitive phrases 1 to n in the second row all correspond to the deletion identifier "Delete".

Table 1

Update-operation identifier	Sensitive phrase 1	Sensitive phrase 2	...	Sensitive phrase n
Add	xxx	yyy	...	zzz
Delete	mmm	nnn		ttt

[0032] A form of the comment and a quantity of sensitive phrases in the comment are not specifically limited in embodiments of the present disclosure. The supervisory node device may alternatively add the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier to another field in the piece of transaction data. Positions at which the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier are located in the piece of transaction data are not limited herein.

[0033] The supervisory node device may further encrypt the sensitive phrase corresponding to the update-operation identifier. In one embodiment, the supervisory node device encrypts the sensitive phrase corresponding to the update-operation identifier through a preset encryption algorithm, so as to obtain an encrypted sensitive phrase. The supervisory node device generates the piece of transaction data based on the encrypted sensitive phrase and the update-operation identifier. The preset encryption algorithm is not specifically limited in embodiments of the present disclosure.

[0034] In such case, after the piece of transaction data is stored in the blockchain, a common user without the knowledge of a decryption algorithm cannot decrypt the encrypted sensitive phrase in the piece of transaction data. Wide spread of the sensitive phrase in the piece of transaction data is prevented.

[0035] In step 202, the supervisory node device broadcasts the piece of transaction data in a blockchain system.

[0036] In the step 202, a node device other than the supervisory node device may be enabled to receive the piece of transaction data.

[0037] In step 203, a node device receives the piece of transaction data.

[0038] It is appreciated that that all node devices in the blockchain may receive the piece of transaction data.

[0039] In step 204, the node device checks the piece of transaction data.

[0040] The node device is a node device other than the supervisory node device in the blockchain system. The node device may check a piece of transaction data by checking the update-operation identifier carried in the piece of transaction data. The piece of transaction data is verified in a case that the update-operation identifier carried in the piece of transaction data is verified. Otherwise, the piece of transaction data fails the verification.

[0041] It is appreciated that some of the node devices in the blockchain may not check the piece of transaction data, and such devices would not package the piece of transaction data into a block.

[0042] In one embodiment, the piece of transaction data is verified in a case that a form of the update-operation identifier carried in the piece of transaction data is verified. Otherwise, the piece of transaction data fails the verification. For example, "Add" serves as the addition identifier, and "Delete" serves as the deletion identifier. In such case, the piece of transaction data is verified in a case that the update-operation identifier carried in the piece of transaction data is "Add" or "Delete". Otherwise, the piece of transaction data fails the verification.

[0043] When the piece of transaction data carries the supervision identifier, the node device may check the piece of transaction data by checking the supervision identifier carried in the piece of transaction data. The piece of transaction data is verified in a case that the supervision identifier carried in the piece of transaction data is verified. Otherwise, the piece of transaction data fails the verification.

[0044] The node device may check the supervision identifier in a target piece of transaction data through either a first manner or a second manner.

[0045] In the first manner, the node device checks the supervision identifier carried in the piece of transaction data, by using supervision information of the supervisory node device. The supervision information is stored in a genesis block in the blockchain deployed on the node device.

[0046] The supervision information includes public keys of all supervisory node devices or addresses of all supervisory node devices in the blockchain system, and is configured to indicate an identity of a node device with supervisory authority. In an initialing phase of the blockchain system, the supervision information of the supervisory node device may be stored in the genesis

block, so that each node device in the blockchain system is aware of which node device has supervisory authority.

[0047] In one embodiment, the supervision identifier carried in the piece of transaction data is a signature of a supervisory node device. The supervision identifier is verified in a case that a public key of the supervisory node device is stored in the genesis block of the blockchain deployed on the node device. Otherwise, the supervision identifier fails the verification.

[0048] In one embodiment, the supervision identifier carried in the piece of transaction data is an address of a supervisory node device. The supervision identifier is verified in a case that the address of the supervisory node device is stored in the genesis block of the blockchain deployed on the node device. Otherwise, the supervision identifier fails the verification.

[0049] In the second manner, the node device checks the supervision identifier in the piece of transaction data by executing a first contract.

[0050] The first contract is a smart contract configured to verify the supervision identifier in the blockchain system. The node device may be triggered to execute the first contract in response to receiving a piece of transaction data carrying the supervision identifier, so as to check the supervision identifier carried in the piece of transaction data.

[0051] In one embodiment, the supervision identifier in the piece of transaction data is a signature of a supervisory node device. The supervision identifier is verified in a case that a public key of the supervisory node device is stored in the first contract. Otherwise, the supervision identifier fails the verification.

[0052] In one embodiment, the supervision identifier in the piece of transaction data is an address of a supervisory node device. The supervision identifier is verified in a case that the address of the supervisory node device is stored in the first contract. Otherwise, the supervision identifier fails the verification.

[0053] The node device in the blockchain system verifies the piece of transaction data by using the supervision identifier, such that all the transaction data carrying the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier is generated by the supervisory node device in the blockchain. Thereby, the credibility of the transaction data carrying the update-operation identifier and the sensitive phrase is ensured in the blockchain system.

[0054] In step 205, the node device stores a target block including the piece of transaction data into a blockchain of the blockchain system, in a case that a consensus is reached in the blockchain system on the piece of transaction data.

[0055] In an optional embodiment, the step 205 may be performed after the step 204. It is appreciated that that a node device is capable to perform the step 205 only when it has performed the step 204. When a majority of node devices in the blockchain system have verified the piece of transaction data, it may be considered that the consensus is reached in the blockchain system on the piece of transaction data. In one embodiment, the step 205 may be implemented in a process including following steps 205A and 205B.

[0056] In step 205A, the node device packages the piece of transaction data into the target block, in a case that multiple node devices in the blockchain system verify the piece of transaction data.

[0057] In some embodiments, a target identifier may be added into the target block when the node device in the blockchain system packages the piece of transaction data, which carry the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier, into the target block. Thereby, a node device in the blockchain system is capable to obtain the target block from the blockchain based on the target identifier. The target identifier is not specifically limited in this embodiment.

[0058] In step 205B, the node device stores the target block into the blockchain deployed on the node device, in a case that a consensus is reached on the target block among the multiple node devices in the blockchain system.

[0059] In a case that the multiple node devices in the blockchain system verify the target block, the consensus is reached on the target block among the multiple node devices. Each node device in the blockchain system may check the target block through an attribute of the target block. The attribute of the target block include a block number, a Merkle root, a quantity of pieces of transaction data in the block, or the like.

[0060] In one embodiment, the target block is verified by the node device in a case that the attribute of the target block meets a condition for being added into the blockchain. Otherwise, the target block fails the verification. For example, the target block is verified by the node device in a case that a block number of the target block is equal to one plus that of the last block in the blockchain deployed on the node device.

[0061] In step 206, a node device obtains the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier from the target block including the piece of transaction data, in a case that the target block is stored into the blockchain of the blockchain system.

[0062] It is appreciated that that all node devices in the blockchain may perform the step 206. The node device may obtain the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier from the target block. In one embodiment, the step 206 may be implemented through either a third manner or a fourth manner.

[0063] In the third manner, the node device obtains at least one piece of transaction data from the target block. In a case that one of the at least one piece of transaction data carries an update-operation identifier, the node device obtains the update-operation identifier and the sensitive phrase from data content of such piece of transaction data.

[0064] In one embodiment, the node device may examine content of comment fields of all transaction data in the target block. In a case that an update-operation identifier is detected from a comment field of a piece of transaction data in the target block, the node device obtains data content in the comment field of such piece of transaction data as the update-operation identifier and the sensitive phrase.

[0065] In the fourth manner, the node device obtains at least one piece of transaction data from the target block. In a case that one of the at least on piece of transaction data carries a supervision identifier, the node device obtains the update-operation identifier and the sensitive phrase from data content of such piece of transaction data.

[0066] In one embodiment, the node device may query initiator addresses of all transaction data in the target block. In a case that an initiator address of a piece of transaction data is found as an address of the supervisory node devices stored in the genesis block, the node device obtains the update-operation identifier and the sensitive phrase from the data content of such piece of transaction data.

[0067] In one embodiment, the node device may query signatures of all transaction data in the target block. In a case that a signature of a piece of transaction data is found to correspond to a public key of the supervisory node device stored in the genesis block, the node device obtains the update-operation identifier and the sensitive phrase from the data content of such piece of transaction data.

[0068] The node device needs to obtain the target block from the blockchain deployed the node device, before obtaining the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier from the target block. The node device may obtain the target block from the blockchain through either a fifth manner or a sixth manner.

[0069] In the fifth manner, transaction data in a block is detected in response to the block being stored into the blockchain deployed on the node device. In a case that a piece of transaction data in the block carries an update-operation identifier or a supervision identifier, the node device obtains such block as the target block.

[0070] Alternatively, the node device may not perform the real-time detection on blocks in the blockchain. In one embodiment, the node device examines periodically at least one piece of transaction data in at least one block, which is newly stored during the last preset period into the blockchain deployed on the node device. In a case that a piece of transaction data in a block carries an update-operation identifier or a supervision identifier, such block is obtained as the target block. For example, the node device detects every hour at least one piece of transaction data in at least one block, which is newly stored during the last hour into the blockchain deployed on the node device. In a case that a piece of transaction data in a block carries an update-operation identifier or a supervision identifier, such block is obtained as the target block.

[0071] In the sixth manner, the node device obtains a block from the blockchain as the target block in case of detecting that the block carries a target identifier. The target identifier is configured to indicate that the block carries the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier.

[0072] In step 207, the node device updates a database of sensitive phrases according to the update-operation identifier and the sensitive phrase in the target block.

[0073] The update-operation identifier in the piece of transaction data may be an addition identifier or a deletion identifier. Hence, in case of different update-operation identifiers, the node device updates the database of sensitive phrases with the sensitive phrase in different manners.

[0074] In one embodiment, the node device adds a sensitive phrase corresponding to the addition identifier into the database of sensitive phrases, in a case that the update-operation identifier in the piece of transaction data is an addition identifier. Table 1 illustrated in the step 201 is further taken as an example. The sensitive phrases 1 to n in the first row of Table 1 all correspond to the addition identifier "Add". Hence, the node device adds the sensitive phrases 1 to n in the first row of Table 1 into the database of sensitive phrases.

[0075] The sensitive phrase corresponding to the addition identifier may or may not exist in the database of sensitive phrases, before the node device updates the database of sensitive phrases. The node device adds the sensitive phrase corresponding to the addition identifier into the database of sensitive phrases, in a case that such sensitive phrase does not exist in the database of sensitive phrases.

[0076] In one embodiment, the update-operation identifier in the piece of transaction data is the addition identifier, and the node device searches the database of sensitive phrases for the sensitive phrase corresponding to the addition identifier. The node device adds the sensitive phrase corresponding to the addition identifier into the database of sensitive phrases, in a case that the sensitive phrase corresponding to the addition identifier is not included in the database of sensitive phrases. The node device may not perform the adding operation, in a case that the sensitive phrase corresponding to the addition identifier is included in the database of sensitive phrases.

[0077] In one embodiment, the node device deletes a sensitive phrase corresponding to the deletion identifier from the database of sensitive phrases, in a case that the update-operation identifier in the piece of transaction data is a deletion identifier. Table 1 illustrated in the step 201 is further taken as an example. The sensitive phrases 1 to n in the second row of Table 1 all correspond to the deletion identifier "Delete". Hence, the node device deletes the sensitive phrases 1 to n in the second row of Table 1 from the database of sensitive phrases.

[0078] The node device may further set a weight for a sensitive phrase in the database of sensitive phrases, in order to indicate the sensitivity of the sensitive phrase. The greater the weight of the sensitive phrase is, the higher the sensitivity of the sensitive phrase is. The smaller the weight of the sensitive phrase is, the lower the sensitivity of the sensitive phrase is. The node device increases the weight of a sensitive phrase corresponding to the addition identifier, in a case the sensitive phrase exists in the database of sensitive phrases.

[0079] The weight of the sensitive phrase may be determined based on times of the adding operation performed on the sensitive phrase. In one embodiment, the node device increases the weight of each sensitive phrase by a preset value, each time the node device obtains an addition identifier corresponding to such sensitive phrase.

[0080] In a case that the sensitive phrase obtained by the node device from the target block is an encrypted sensitive phrase, the node device may decrypt the encrypted sensitive phrase through a preset decryption algorithm, so as to obtain a decrypted sensitive phrase. The node device then updates the database of sensitive phrases with the decrypted sensitive phrase. The

preset decryption algorithm corresponds to a preset encryption algorithm for encrypting the sensitive phrase.

[0081] In the method according to embodiments of the present disclosure, the node device in the blockchain system may verify the piece of transaction data carrying the sensitive phrase, and the target block including the piece of transaction data may be stored into the blockchain. In such case, each node device in the blockchain system may obtain the sensitive phrase from the target block in the blockchain of the blockchain system, and update the database of sensitive phrases thereof according to the update-operation identifier corresponding to the sensitive phrase. Thereby, the database of sensitive phrases on each node device can be synchronously updated. In addition, the node device in the blockchain system verifies the piece of transaction data by using the supervision identifier, so that all transaction data carrying the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier in the blockchain is generated by the supervisory node device. Thereby, credibility of the transaction data carrying the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier on the blockchain is ensured. Further, weights are set for the sensitive phrases in the database of sensitive phrases. The sensitivity of the sensitive phrases is indicated by the weights of the sensitive phrases, such that the sensitivity of the sensitive phrases is directly represented by quantified data, facilitating subsequent operations based on the database of sensitive phrases, such as data queries. Moreover, each time storing a target block, the node device may obtain the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier from the target block. Thereby, each node device can update the database of sensitive phrases thereof in real time. It is avoided that the node device cannot accurately filter content of a to-be-queried block due to the database of sensitive phrases not timely updated. Further, the sensitive phrase in the piece of transaction data may be encrypted, such that a common user without the knowledge of the decryption algorithm cannot decrypt the encrypted sensitive phrase in the piece of transaction data. Thereby, wide spread of the sensitive phrase in the piece of transaction data is prevented.

[0082] The node device in Figure 2 stores the database of sensitive phrases locally, so that the node device can filter the content of the to-be-queried block according to the database of sensitive phrases. Reference is made to Figures 3 for illustrating a process of data query at the node device based on the database of sensitive phrases. Figure 3 is a flowchart of a method for data query based on data synchronization according to an embodiment of the present disclosure. In a specific embodiment, the method includes following steps 301 to 305.

[0083] In step 301, a node device receives a query request. The query request carries a block number of a to-be-queried block.

[0084] The node device may be any node device in the blockchain system. The block number may be a number of the block in the blockchain deployed in the blockchain system, or may be a block height, for example, a block 001 or a block 002.

[0085] In step 302, the node device determines a block corresponding to the block number in a blockchain of a blockchain system, according to the block number carried in the query request.

[0086] The node device may determine the block corresponding to the block number carried in the query request, by searching block numbers of all blocks in the blockchain deployed on the node device. In one embodiment, a block to which a block number belongs is obtained as a first target block, in a case that such block number is found in the blockchain deployed on the node device and is same as the block number carried in the query request. The first target block is the block determined by the node device.

[0087] In step 303, the node device parses the determined block, to obtain at least one piece of transaction data from the block.

[0088] In step 304, the node device compares the at least one piece of transaction data from the block with a sensitive phrase in a database of sensitive phrases.

[0089] The node device may perform the comparison based on weights of the sensitive phrases. In one embodiment, the node device compares multiple sensitive phrases in the database of sensitive phrases, one by one in a descending order of weights, with the at least one piece of transaction data in the block. The weight is determined based on how many times the adding operation is performed on the sensitive phrase.

[0090] The node device obtains the weights of the sensitive phrases in the database of sensitive phrases before the comparison, then sorts the sensitive phrases based on weights in the descending order, and finally compares the sorted sensitive phrases sequentially with the at least one piece of transaction data in the block.

[0091] For example, there are three sensitive phrases in the database of sensitive phrases. The weight of a sensitive phrase A is 1, the weight of a sensitive phrase B is 2, and the weight of a sensitive phrase C is 3. The node device sorts the sensitive phrases in the database of sensitive phrases as: the sensitive phrase C, the sensitive phrase B, and the sensitive phrase A. Hence, the node device first compares at least one piece of transaction data in the block with the sensitive phrase C, then compares the at least one piece of transaction data in the block with the sensitive

phrase B, and finally compares the at least one piece of transaction data in the block with the sensitive phrase A.

[0092] In step 305, the node device filters a first piece of transaction data by screening the sensitive phrase in the database of sensitive phrases, to obtain query feedback information, in a case that the at least one piece of transaction data includes the first piece of transaction data. The query feedback information includes the filtered at least one piece of transaction data. The first piece of transaction data includes any sensitive phrase in the database of sensitive phrases.

[0093] The node device may screen the sensitive phrase in the transaction data by deleting the sensitive phrase or replacing the sensitive phrase. In such case, the step 305 may be implemented through either a seventh manner or an eighth manner.

[0094] In the seventh manner, the node device deletes the sensitive phrase in the database of sensitive phrases from the first piece of transaction data to obtain the query feedback information, in a case that the at least one piece of transaction data includes the first piece of transaction data. The query feedback information includes the at least one piece of transaction data subject to the deletion.

[0095] For example, the first piece of transaction data carries the sensitive phrase A in the database of sensitive phrases, and the node device deletes the sensitive phrase A from the first piece of transaction data. Accordingly, the first piece of transaction data in the obtained query feedback information is the first piece of transaction data subject to the deletion.

[0096] In the eighth manner, the node device replaces the sensitive phrase in the first piece of transaction data with a target warning phrase to obtain the query feedback information, in a case that the at least one piece of transaction data includes the first piece of transaction data. The query feedback information includes at least one piece of transaction data obtained subject to the replacement.

[0097] The target warning phrase may be represented by a character string, such as "******" or "the information here is sensitive information", configured to indicate the sensitive phrase. Content of the target warning phrase is not specifically limited in this embodiment.

[0098] For example, the first piece of transaction data carries the sensitive phrase A in the database of sensitive phrases, and the node device replaces the sensitive phrase A in the first piece of transaction data with the target warning phrase "******". Accordingly, the first piece of transaction data in the obtained query feedback information is the first piece of transaction data subject to the replacement.

[0099] The node device may further display the query feedback information on a display interface of the node device, to facilitate view of the user. A specific form of displaying the query feedback information is not limited in embodiments of the present disclosure.

[0100] Hereinabove described is a process of the node device filtering the to-be-queried block to screen the sensitive phrase based on the local database of sensitive phrases. Alternatively, in one embodiment, the node device may screen the sensitive phrase in the to-be-queried block by executing a smart contract in the blockchain system. The smart contract for screening the sensitive phrases in the to-be-queried block is not specifically limited in embodiments of the present disclosure. The smart contract may be maintained by a user with supervisory authority without help from other node devices.

[0101] In the method according to embodiments of the present disclosure, the transaction data in the to-be-queried block is compared with the sensitive phrase in the database of sensitive phrases, and the transaction data carrying the sensitive phrase in the to-be-queried block is filtered. Thereby, the node device displays the filtered transaction data to the user. Each node device in the blockchain system stores a database of sensitive phrases, so that each node device in the blockchain system can screen the sensitive phrase in the to-be-queried block based on the database of sensitive phrases thereof. Hence, the wide spread of sensitive phrases is prevented in the blockchain. In addition, the node device in the blockchain system may screen the sensitive phrase in the to-be-queried block by executing the smart contract. In such case, only the user with supervisory authority is required to maintain the smart contract, and other node devices is not necessary in the maintenance, reducing a service load on the other node devices. Moreover, the node device filters to-be-queried data only according to the local database of sensitive phrases, thereby avoiding high time cost and improving filtering efficiency of the node device.

[0102] Any combination of the foregoing optional technical solutions may serve as an optional embodiment of the present disclosure. Such combination is not enumerated herein.

[0103] Figure 4 is a schematic structural diagram of an apparatus for data synchronization according to an embodiment of the present disclosure. Reference is made to Figure 4, where the apparatus includes a receiving module 401, an obtaining module 402, and an update module 403. Modules included in the apparatus for data synchronization may be entirely or partially implemented through software, hardware, or a combination thereof.

[0104] The receiving module 401 is coupled to the obtaining module 402. The receiving module 401 is configured to receive a piece of transaction data. The piece of transaction data

carrying an update-operation identifier and a sensitive phrase corresponding to the update-operation identifier.

[0105] The obtaining module 402 is coupled to the update module 403. The obtaining module 402 is configured to obtain the update-operation identifier and the sensitive phrase from a target block including the piece of transaction data, in a case that the target block is stored into a blockchain of a blockchain system.

[0106] The update module 403 is configured to update a database of sensitive phrases according to the update-operation identifier and the sensitive phrase from the target block.

[0107] In an optional embodiment, the update module 403 includes an addition unit or a deletion unit.

[0108] The addition unit is configured to add a sensitive phrase corresponding to an addition identifier into the database of sensitive phrases, in a case that the update-operation identifier in the piece of transaction data is the addition identifier.

[0109] The deletion unit is configured to delete a sensitive phrase corresponding to a deletion identifier from the database of sensitive phrases, in a case that the update-operation identifier in the piece of transaction data is the deletion identifier.

[0110] In an optional embodiment, the addition unit is configured to: search the database of sensitive phrases for the sensitive phrase corresponding to the addition identifier, in a case that the update-operation identifier in the piece of transaction data is the addition identifier; and add the sensitive phrase corresponding to the addition identifier into the database of sensitive phrases, in a case that the sensitive phrase corresponding to the addition identifier is not included in the database of sensitive phrases.

[0111] In an optional embodiment, the obtaining module 402 is configured to obtain data content of a piece of transaction data in the target block, as the update-operation identifier and the sensitive phrase, in a case that the piece of transaction data in the target block carries a supervision identifier.

[0112] In an optional embodiment, the supervision identifier includes a signature of the supervisory node device or an address of the supervisory node device.

[0113] In an optional embodiment, the apparatus further includes a determination module, a comparison module, and a filtering module.

[0114] The determination module is configured to determine a block corresponding to a block number carried in a query request, in the blockchain of the blockchain system and according to the block number.

[0115] The comparison module is configured to compare at least one piece of transaction data in the block corresponding to the block number, with a sensitive phrase in the database of sensitive phrases.

[0116] The filtering module is configured to filter a first piece of transaction data by screening the sensitive phrase in the database of sensitive phrases, to obtain query feedback information, in a case that the at least one piece of transaction data includes the first piece of transaction data. The query feedback information includes the at least one piece of transaction data obtained subject to the filtering, and the first piece of transaction data includes the sensitive phrase in the database of sensitive phrases.

[0117] In an optional embodiment, the comparison module is configured to compare multiple sensitive phrases in the database of sensitive phrases, one by one in an descending order of weights of the sensitive phrases, with the at least one piece of transaction data in the block. The weight is determined according to times of an adding operation performed on the corresponding sensitive phrase.

[0118] In an optional embodiment, the filtering module is configured to delete the sensitive phrase in the database of sensitive phrases from the first piece of transaction data, to obtain the query feedback information, in a case that the at least one piece of transaction data includes the first piece of transaction data. The query feedback information includes the at least one piece of transaction subject to the deleting.

[0119] Alternatively, the filtering module is configured to replace the sensitive phrase in the first piece of transaction data with a target warning phrase, to obtain the query feedback information, in a case that the at least one piece of transaction data includes the first piece of transaction data. The query feedback information includes the at least one piece of transaction data subject to the replacing.

[0120] In the apparatus according to embodiments of the present disclosure, the node device in the blockchain system may verify the piece of transaction data carrying the sensitive phrase, and the target block including the piece of transaction data may be stored into the blockchain. In such case, each node device in the blockchain system may obtain the sensitive phrase from the target block in the blockchain of the blockchain system, and update the database of sensitive phrases

thereof according to the update-operation identifier corresponding to the sensitive phrase. Thereby, the database of sensitive phrases on each node device can be synchronously updated. In addition, the node device in the blockchain system verifies the piece of transaction data by using the supervision identifier, so that all transaction data carrying the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier in the blockchain is generated by the supervisory node device. Thereby, credibility of the transaction data carrying the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier on the blockchain is ensured. Moreover, each time storing a target block, the node device may obtain the update-operation identifier and the sensitive phrase corresponding to the update-operation identifier from the target block. Thereby, each node device can update the database of sensitive phrases thereof in real time. It is avoided that the node device cannot accurately filter content of a to-be-queried block due to the database of sensitive phrases not timely updated. Further, the transaction data in the to-be-queried block is compared with the sensitive phrase in the database of sensitive phrases, and the transaction data carrying the sensitive phrase in the to-be-queried block is filtered. Thereby, the node device displays the filtered transaction data to the user. Each node device in the blockchain system stores a database of sensitive phrases, so that each node device in the blockchain system can screen the sensitive phrase in the to-be-queried block based on the database of sensitive phrases thereof. Hence, the wide spread of sensitive phrases is prevented in the blockchain. In addition, the node device in the blockchain system may screen the sensitive phrase in the to-be-queried block by executing the smart contract. In such case, only the user with supervisory authority is required to maintain the smart contract, and other node devices is not necessary in the maintenance, reducing a service load on the other node devices.

[0121] It is merely an example that the apparatus for data synchronization is divided into the aforementioned functional modules when performing data synchronization in the foregoing embodiments. In practice, the aforementioned functions may be allocated to and implemented by different functional modules on requirement. That is, an internal structure of the apparatus may be divided into different functional modules, to achieve all or some of the aforementioned functions. In addition, the foregoing apparatus embodiments are based on the same concept as the foregoing method embodiments. A specific implementation process of the apparatus embodiments may refer to that of the method embodiments.

[0122] Figure 5 is a schematic structural diagram of a computer device according to an embodiment of the present disclosure. Specifically, the computer device may be a node device as shown in Figure 1. The node device 500 may vary due to different configurations or performances, and may include one or more central processing units (CPUs) 501 and one or more memories 502.

The memory 502 stores at least one instruction, and the at least one instruction is loaded and executed by the processor 501 to implement the method according to the foregoing embodiments. The node device may further include components such as a wired or wireless network interface, a keyboard, and an input/output (I/O) interface, to facilitate input and output. The node device may further include another component configured to implement a function of a device. Details are not described herein.

[0123] In one embodiment, a computer-readable storage medium, such as a memory including instructions, is further provided. The instructions may be executed by a processor in a terminal, so as to complete the method for data synchronization or the method for data query according to the foregoing embodiments.

[0124] In one embodiment, a computer device is provided, including a memory and a processor. The memory stores computer-readable instructions, and the computer-readable instructions when executed by the processor configure the processor to perform steps in the foregoing method for data synchronization. The foregoing method for data synchronization may refer to the foregoing embodiments.

[0125] In one embodiment, a computer-readable storage medium is provided. The computer-readable storage medium stores computer-readable instructions, and the computer-readable instructions when executed by a processor configure the processor to perform steps in the foregoing method for data synchronization. The foregoing method for data synchronization may refer to the foregoing embodiments.

[0126] Those skilled in the art may understand that all or some procedures in the foregoing method embodiments may be implemented by computer-readable instructions instructing relevant hardware. A program may be stored in a non-volatile computer-readable storage medium. When the program is executed, the procedures of the foregoing method embodiments may be implemented. Each memory, storage, database, or another medium to which the embodiments of the present disclosure refer may include a non-volatile or a volatile memory. The non-volatile memory may include a read-only memory (ROM), a programmable ROM (PROM), an electrically programmable ROM (EPROM), an electrically erasable programmable ROM (EEPROM), or a flash memory. The volatile memory may include a random access memory (RAM) or an external cache. As description rather than limitation, the RAM may be implemented in various forms, such as a static RAM (SRAM), a dynamic RAM (DRAM), a synchronous DRAM (SDRAM), a double data rate SDRAM (DDRSDRAM), an enhanced SDRAM (ESDRAM), a synchlink (Synchlink) DRAM

(SLDRAM), a rambus (Rambus) direct RAM (RDRAM), a direct rambus dynamic RAM (DRDRAM), or a rambus dynamic RAM (RDRAM).

[0127] The technical features in the foregoing embodiments may be variously combined. For concise description, the possible combinations of the technical features in the embodiments are not enumerated. A combination of the technical features should be considered as falling within the protection scope of the present disclosure, as long as the technical features in the combination do not conflict with each other,.

[0128] The foregoing embodiments merely describe several implementations of the present disclosure in detail, and should not be construed as a limitation to the patent scope of the present disclosure. Those skilled in the art can make several variations and improvements without departing from the idea of the present disclosure. These variations and improvements also fall within the protection scope of the present disclosure. Therefore, the protection scope of the patent of the present disclosure should be subject to the appended claims.

AMENDED CLAIMS

What is claimed is:

1. A method for data synchronization, performed by a computer device, wherein the method comprises:

receiving a piece of transaction data, wherein the piece of transaction data carries an update-operation identifier and a sensitive phrase corresponding to the update-operation identifier, wherein the update-operation identifier indicates an update operation to be performed by the computer device with respect to the sensitive phrase;

obtaining the update-operation identifier and the sensitive phrase from a target block comprising the piece of transaction data, in a case that the target block is stored into a blockchain of a blockchain system; and

updating a database of sensitive phrases according to the update-operation identifier and the sensitive phrase from the target block, wherein the database is locally stored at the computer device and serves as a basis for the computer device filtering content of a block queried at the computer device.

2. The method according to claim 1, wherein updating the database of sensitive phrases according to the update-operation identifier and the sensitive phrase from the target block comprises:

adding a sensitive phrase corresponding to an addition identifier into the database of sensitive phrases, in a case that the update-operation identifier in the piece of transaction data is the addition identifier; or

deleting a sensitive phrase corresponding to a deletion identifier from the database of sensitive phrases, in a case that the update-operation identifier in the piece of transaction data is the deletion identifier.

3. The method according to claim 2, wherein adding the sensitive phrase corresponding to the addition identifier into the database of sensitive phrases in the case that the update-operation identifier in the piece of transaction data is the addition identifier comprises:

searching the database of sensitive phrases for the sensitive phrase corresponding to the addition identifier, in the case that the update-operation identifier in the piece of transaction data is the addition identifier; and

adding the sensitive phrase corresponding to the addition identifier into the database of sensitive phrases, in a case that the sensitive phrase corresponding to the addition identifier is not comprised in the database of sensitive phrases.

4. The method according to claim 1, wherein obtaining the update-operation identifier and the sensitive phrase from the target block comprises:

obtaining the update-operation identifier and the sensitive phrase data from a piece of transaction data in the target block, in a case that the piece of transaction data in the target block carries a supervision identifier.

5. The method according to claim 4, wherein the supervision identifier comprises a signature of the supervisory node device or an address of the supervisory node device.

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

determining a block corresponding to a block number carried in a query request, in the blockchain of the blockchain system and according to the block number;

comparing at least one piece of transaction data in the block corresponding to the block number, with a sensitive phrase in the database of sensitive phrases; and

filtering a first piece of transaction data by screening the sensitive phrase in the database of sensitive phrases, to obtain query feedback information, in a case that the at least one piece of transaction data comprises the first piece of transaction data;

wherein the query feedback information comprises the at least one piece of transaction data obtained subject to the filtering, and the first piece of transaction data comprises the sensitive phrase in the database of sensitive phrases.

7. The method according to claim 6, wherein comparing the at least one piece of transaction data in the block corresponding to the block number with the sensitive phrase in the database of sensitive phrases comprises:

comparing a plurality of sensitive phrases in the database of sensitive phrases, one by one in an descending order of weights of the plurality of sensitive phrases, with the at least one piece of transaction data in the block,

wherein the weight is determined according to times of an adding operation performed on the corresponding sensitive phrase.

8. The method according to claim 6, wherein filtering the first piece of transaction data by screening the sensitive phrase in the database of sensitive phrases to obtain the query feedback

information, in the case that the at least one piece of transaction data comprises the first piece of transaction data, comprises:

deleting the sensitive phrase in the database of sensitive phrases from the first piece of transaction data to obtain the query feedback information, in the case that the at least one piece of transaction data comprises the first piece of transaction data, wherein the query feedback information comprises the at least one piece of transaction subject to the deleting; or

replacing the sensitive phrase in the first piece of transaction data with a target warning phrase to obtain the query feedback information, in a case that the at least one piece of transaction data comprises the first piece of transaction data, wherein the query feedback information comprises the at least one piece of transaction data subject to the replacing.

9. An apparatus for data synchronization, comprising:

a receiving module, configured to receive a piece of transaction data, wherein the piece of transaction data carries an update-operation identifier and a sensitive phrase corresponding to the update-operation identifier, wherein the update-operation identifier indicates an update operation to be performed by the computer device with respect to the sensitive phrase;

an obtaining module, configured to obtain the update-operation identifier and the sensitive phrase from a target block comprising the piece of transaction data, in a case that the target block is stored into a blockchain of a blockchain system; and

an update module, configured to update a database of sensitive phrases according to the update-operation identifier and the sensitive phrase from the target block, wherein the database is locally stored at the computer device and serves as a basis for the computer device filtering content of a block queried at the computer device.

10. The apparatus according to claim 9, wherein the update module comprises:

an addition unit, configured to add a sensitive phrase corresponding to an addition identifier into the database of sensitive phrases, in a case that the update-operation identifier in the piece of transaction data is the addition identifier; or

a deletion unit, configured to delete a sensitive phrase corresponding to a deletion identifier from the database of sensitive phrases, in a case that the update-operation identifier in the piece of transaction data is the deletion identifier.

11. The apparatus according to claim 10, wherein the addition unit is configured to:

search the database of sensitive phrases for the sensitive phrase corresponding to the addition

identifier, in the case that the update-operation identifier in the piece of transaction data is the addition identifier, and

add the sensitive phrase corresponding to the addition identifier into the database of sensitive phrases, in a case that the sensitive phrase corresponding to the addition identifier is not comprised in the database of sensitive phrases.

12. The apparatus according to claim 9, wherein the obtaining module is configured to obtain the update-operation identifier and the sensitive phrase data from a piece of transaction data in the target block, in a case that the piece of transaction data in the target block carries a supervision identifier.

13. The apparatus according to claim 9, further comprising:

a determination module, configured to determine a block corresponding to a block number carried in a query request, in the blockchain of the blockchain system and according to the block number;

a comparison module, configured to compare at least one piece of transaction data in the block corresponding to the block number, with a sensitive phrase in the database of sensitive phrases; and

a filtering module, configured to filter a first piece of transaction data by screening the sensitive phrase in the database of sensitive phrases, to obtain query feedback information, in a case that the at least one piece of transaction data comprises the first piece of transaction data;

wherein the query feedback information comprises the at least one piece of transaction data obtained subject to the filtering, and the first piece of transaction data comprises the sensitive phrase in the database of sensitive phrases.

14. A computer device, comprising a memory and a processor, wherein the memory stores computer-readable instructions, and the computer-readable instructions when executed by the processor configure the processor to perform the method according to any one of claims 1 to 8.

15. A non-volatile storage medium, storing computer-readable instructions, wherein the computer-readable instructions when executed by one or more processors configured the one or more processors to perform the method according to any one of claims 1 to 8.