BLOCKCHAIN-BASED DATA VERIFICATION SYSTEM AND METHOD, COMPUTING DEVICE AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] The present specification relates to the field of blockchain technologies, and in particular, to a blockchain-based data verification system and method, a computing device and a storage medium.

BACKGROUND

[0002] With the development of Internet technologies, financial institutions and transaction platforms are becoming more diverse. Therefore, transaction data between financial institutions or between a transaction platform and a financial institution needs to be verified regularly to identify data differences of a same transaction in different institutions.

[0003] In the existing technologies, a data processing method between institutions is that institution A packages and sends transaction data generated in a predetermined time period to institution B, and institution B verifies the data in the file package. However, development costs of verification methods used in the existing technologies are high, involving data export from a core service system, file transmission, and data comparison with the core service system. It will take a long time to complete a whole process if a transaction volume in a verification cycle is large, resulting in poor timeliness. Therefore, it is difficult to achieve real-time or on-time verification, and there is a lack of an arbitration mechanism, for data verified in an existing way, that can be recognized by both parties if there is a dispute in the future.

SUMMARY

[0004] In view of the above, implementations of the present specification provide a blockchain-based data verification system and method, a computing device and a

storage medium, so as to overcome technical deficiencies existing in the existing technologies.

[0005] According to a first aspect of some implementations of the present specification, a blockchain-based data verification system is provided, including: a first verification system, a second verification system, and a first blockchain node and a second blockchain on a blockchain network, where the first verification system is configured to: collect first service data based on a predetermined condition and generate a first verification file including the first service data, and send a verification request to the second verification system, the verification request including the first verification file; the second verification system is configured to: receive the verification request, verify the first service data in the first verification file with second service data in a local database of the second verification system and generate a verification result notification, send the verification result notification to the first verification system, and send successfully verified second service data in the local database to the first blockchain node on the blockchain network; the first verification system is further configured to: receive the verification result notification, and send successfully verified first service data to the second blockchain node on the blockchain network; the first blockchain node corresponds to a node of the blockchain network and is configured to receive and store the successfully verified second service data that is sent by the second verification system; and the second blockchain node corresponds to a node of the blockchain network and is configured to receive and store the successfully verified first service data that is sent by the first verification system.

[0006] Optionally, the blockchain-based data verification system further includes a first service system and a second service system; the first service system is configured to send the first service data to the first verification system, and the first service data includes, for a piece of data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data; the second service system is configured to send the second service data to the second verification system, and the second service data includes, for a piece of data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data; and the second verification system is further configured to receive the second service data of the second service system and store the second service data in the local database.

[0007] Optionally, the second verification system is further configured to: determine a verification rule corresponding to the second service data based on the second service data, determine a mapping relationship between the second service data and the verification rule, and store the mapping relationship between the second service data and the verification rule in the local database.

[0008] Optionally, the first verification system is further configured to: obtain the first service data, store N pieces of the first service data as the first verification file in response to a number of pieces of the first service data reaching a predetermined threshold N and process the first verification file to generate a first digital digest, and send the verification request to the second verification system, the verification request including the first verification file and the first digital digest corresponding to the first verification file.

[0009] Optionally, the second verification system is further configured to: receive the verification request, extract the first digital digest from the verification request, and validate the first service data in the first verification file based on the first digital digest; and in response to the validating the first service data succeeding, determine the second service data corresponding to the first service data based on the identification information in the first service data, obtain the verification rule corresponding to the critical service information in the second service data, verify the first service data with the second service data in the local database based on the verification rule and generate the verification result notification, and send the verification result notification to the first verification system.

[0010] Optionally, the second verification system is further configured to: verify the first service data with the second service data in the local database based on the verification rule, generate a second verification file based on a result of the verifying the first service data with the second service data and process the second verification file to generate a second digital digest, and send the verification result notification to the first verification system, the verification result notification including the second verification file and the second digital digest corresponding to the second verification file.

[0011] Optionally, the first verification system is further configured to: extract the second verification file and the second digital digest that are included in the verification result notification, validate the second verification file based on the second digital

digest, and in response to the validating the second verification file succeeding, extract and upload the successfully verified first service data in the second verification file to the blockchain network.

[0012] Optionally, the first verification system is further configured to: if unsuccessfully verified first service data exists in the second verification file, update the verification status of the unsuccessfully verified first service data and review or report the unsuccessfully verified first service data.

[0013] According to another aspect of some implementations of the present specification, a blockchain-based data verification method is provided, where the method is applied to a first verification system, and includes: collecting first service data based on a predetermined condition and generating a first verification file including the first service data, the first service data including, for a piece of data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data; sending a verification request to a second verification system, the verification request including the first verification file; and receiving a verification result notification sent by the second verification system, and sending successfully verified first service data to a second blockchain node.

[0014] Optionally, collecting the first service data based on the predetermined condition and generating the first verification file including the first service data includes: obtaining first service data of a first service system; storing N pieces of the first service data as the first verification file in response to a number of pieces of the first service data reaching a predetermined threshold N, and processing the first verification file to generate a first digital digest; and sending the verification request to the second verification system, the verification request including the first verification file and the first digital digest corresponding to the first verification file.

[0015] Optionally, the verification result notification includes a second verification file and a second digital digest corresponding to the second verification file; receiving the verification result notification sent by the second verification system, and sending the successfully verified first service data to the second blockchain node includes: extracting the second verification file and the second digital digest that are included in the verification result notification, and validating the second verification file based on the second digital digest; in response to the validating the second verification file succeeding, extracting and uploading the successfully verified first service data in the

second verification file to the second blockchain node on the blockchain network; and if unsuccessfully verified first service data exists in the second verification file, updating the verification status of the unsuccessfully verified first service data and reviewing or reporting the unsuccessfully verified first service data.

[0016] According to another aspect of some implementations of the present specification, a blockchain-based data verification method is provided, where the method is applied to a second verification system, and includes: obtaining second service data of a second service system and storing the second service data in a local database; receiving a verification request, the verification request including a first verification file; verifying first service data in the first verification file with the second service data in the local database and generating a verification result notification, and sending the verification result notification to a first verification system; and sending successfully verified second service data in the local database to a first blockchain node on a blockchain network.

[0017] Optionally, the method further includes: before receiving the verification request, determining a verification rule corresponding to the second service data based on the second service data; determining a mapping relationship between the second service data and the verification rule; and storing the mapping relationship between the second service data and the verification rule in the local database.

[0018] Optionally, the method further includes: after receiving the verification request of the first service system, extracting a first digital digest from the verification request and validating the first service data in the first verification file based on the first digital digest; and in response to the validating the first service data succeeding, verifying the first service data in the first verification file with the second service data in the local database.

[0019] Optionally, verifying the first service data in the first verification file with the second service data in the local database and generating the verification result notification includes: determining the second service data corresponding to the first service data based on identification information in the first service data; obtaining a verification rule corresponding to critical service information in the second service data; and verifying the first service data with the second service data in the local database based on the verification rule and generating the verification result notification based on a verification result.

[0020] Optionally, generating the verification result notification based on the verification result includes: generating a second verification file based on the verification result; processing the second verification file to generate a second digital digest; and generating the verification result notification based on the second verification file and the second digital digest.

[0021] Optionally, generating the second verification file based on the verification result includes: if all of the first service data in the first verification file is successfully verified, updating a verification status in the first verification file and then generating the second verification file; and if unsuccessfully verified first service data exists in the second verification file, the generated second verification file includes the identification information, the verification status and a verification failure cause that are of each piece of the first service data in the first verification file.

[0022] According to another aspect of some implementations of the present specification, a computing device is provided, including: a memory, a processor, and a computer instruction stored in the memory and executable on the processor, where the steps of the blockchain-based data verification method are implemented when the processor executes the instruction.

[0023] According to another aspect of some implementations of the present specification, a computer-readable storage medium is provided, where the computer-readable storage medium stores a computer instruction, and the steps of the blockchain-based data verification method are implemented when the instruction is executed by a processor.

[0024] In some implementations of the present specification, the verification systems are established outside the service systems, so that a data verification method between institutions is changed as follows: the first service system sends transaction service data to the first verification system, the first verification file is generated in response to the number of pieces of the transaction service data received by the first verification system reaching the predetermined threshold, and the first verification file is sent to the second verification system for data verification. Without affecting normal interaction between the service systems, the data verification is completed through interaction between the verification systems, which improves efficiency of data verification and timeliness. The verified transaction service data is uploaded to the blockchain network, which ensures immutability and credibility of the data.

BRIEF DESCRIPTION OF DRAWINGS

[0025] FIG. 1 is a schematic structural diagram illustrating a blockchain-based data verification system according to some implementations of the present application;

[0026] FIG. 2 is a schematic structural diagram illustrating a blockchain-based data verification system according to some implementations of the present application;

[0027] FIG. 3 is a structural block diagram illustrating a computing device according to some implementations of the present application;

[0028] FIG. 4 is a flowchart illustrating a blockchain-based data verification method according to some implementations of the present application;

[0029] FIG. 5 is a flowchart illustrating a blockchain-based data verification method according to some implementations of the present application; and

[0030] FIG. 6 is a schematic interactive diagram illustrating a blockchain-based data verification method according to some implementations of the present application.

DESCRIPTION OF IMPLEMENTATIONS

[0031] Many specific details are set forth in the following description to facilitate full understanding of the present application. However, the present application can be implemented in many different ways from those described herein, and a person skilled in the art can make similar promotion without departing from the content of the present application, so the present application is not limited to the specific implementations disclosed below.

[0032] The terms used in one or more implementations of the present specification are for the purpose of describing specific implementations only, and are not intended to limit one or more implementations of the present specification. The singular forms of "a", "said" and "the" used in one or more implementations of the present specification and the appended claims are also intended to include plural forms, unless other meanings are clearly indicated in the context. It should be further understood that the term "and/or" used in one or more implementations of the present specification refers to and includes any or all possible combinations of one or more associated listed items.

[0033] It should be understood that although the terms first, second, and the like may be used to describe various kinds of information in one or more implementations of the present specification, such information should not be limited to these terms.

These terms are used only to differentiate information of a same type. For example, the first can also be referred to as the second without departing from the scope of one or more implementations of the present specification, and similarly, the second can also be referred to as the first. Depending on the context, the word "if" used herein can be interpreted as "when" or "while" or "in response to determining".

[0034] The present application provides a blockchain-based data verification system and method, a computing device and a storage medium, which are described in detail one by one in the following implementations.

[0035] FIG. 1 is a schematic structural diagram illustrating a blockchain-based data verification system according to some implementations of the present specification. The system includes: a first verification system 102, a second verification system 104, and a first blockchain node 108 and a second blockchain node 110 on a blockchain network 106.

[0036] The first verification system 102 is configured to: collect first service data based on a predetermined condition and generate a first verification file including the first service data, and send a verification request to the second verification system, the verification request including the first verification file.

[0037] In some implementations of the present specification, the first verification system is further configured to: obtain the first service data, store N pieces of the first service data as the first verification file in response to a number of pieces of the first service data reaching a predetermined threshold N and process the first verification file to generate a first digital digest, and send the verification request to the second verification system, the verification request including the first verification file and the first digital digest corresponding to the first verification file.

[0038] The second verification system 104 is configured to: receive second service data of a second service system and store the second service data in a local database, determine a verification rule corresponding to the second service data based on the second service data, determine a mapping relationship between the second service data and the verification rule, and store the mapping relationship between the second service data and the verification rule in the local database.

[0039] In some implementations of the present specification, the first service data and the second service data are transaction service data of a first service system and the second service system respectively, and the first verification file is a verification file

generated in response to the number of pieces of the first service data obtained by the first verification system reaching N.

[0040] In some implementations of the present specification, the second service data can correspond to one or more verification rules, that is, the second service data and the verification rules can have a one-to-one mapping relationship or a one-to-many mapping relationship, which is not limited in the present specification.

[0041] The second verification system 104 is further configured to: receive the verification request, verify the first service data in the first verification file with the second service data in the local database and generate a verification result notification, send the verification result notification to the first verification system, and send successfully verified second service data in the local database to the first blockchain node on the blockchain network 106.

[0042] In some implementations of the present specification, the second verification system is further configured to: receive the verification request, extract the first digital digest from the verification request, and validate the first service data in the first verification file based on the first digital digest; and in response to the validating the first service data succeeding, determine the second service data corresponding to the first service data based on identification information in the first service data, obtain the verification rule corresponding to critical service information in the second service data, verify the first service data with the second service data in the local database based on the verification rule and generate the verification result notification, and send the verification result notification to the first verification system.

[0043] In some implementations of the present specification, the second verification system is further configured to: verify the first service data with the second service data in the local database based on the verification rule, generate a second verification file based on a result of the verifying the first service data with the second service data and process the second verification file to generate a second digital digest, and send the verification result notification to the first verification system, the verification result notification including the second verification file and the second digital digest corresponding to the second verification file.

[0044] In some implementations of the present specification, the second verification file is a verification file generated by the second verification system based on the verification result after verifying service data in the first verification file.

[0045] The first verification system 102 is further configured to: receive the verification result notification, and send successfully verified first service data to the second blockchain node 110 on the blockchain network 106.

[0046] In some implementations of the present specification, the first verification system is further configured to: if unsuccessfully verified first service data exists in the second verification file, update a verification status of the unsuccessfully verified first service data and review or report the unsuccessfully verified first service data.

[0047] The first blockchain node 108 corresponds to a node of the blockchain network 106 and is configured to receive and store the successfully verified second service data that is sent by the second verification system.

[0048] The second blockchain node 110 corresponds to a node of the blockchain network 106 and is configured to receive and store the successfully verified first service data that is sent by the first verification system.

[0049] In some implementations of the present specification, after receiving successfully verified data, the first blockchain node 108 and the second blockchain node 110 are further configured to: transmit the data to other blockchain nodes, for the blockchain nodes of the blockchain network to reach a consensus on successfully verified service data.

[0050] In practice, the first verification system and the second verification system can be banks, insurance companies, third-party transaction platforms or other transaction service platforms, both the first verification system and the second verification system can verify service data of other relevant service institutions, and data verification is not limited to be performed by two verification systems, and the data verification can be performed by two or more verification systems, which is not limited in the present specification.

[0051] In some implementations of the present specification, timeliness of the data verification can be realized by transmitting transaction data generated by the service systems to the verification systems, and by performing subsequent data verification through the verification systems. Unsuccessfully verified data can be reviewed or reported in time to ensure correctness of the service data. The successfully verified service data can be uploaded to the blockchain nodes by the verification systems, so that the blockchain nodes reach a consensus on the service data and store the service

data in a blockchain of the blockchain network, which ensures authenticity and immutability of the data, and improves credibility of the transaction data.

[0052] FIG. 2 is a schematic structural diagram illustrating a blockchain-based data verification system according to some implementations of the present specification. The system includes: a first service system 202, a first verification system 204, a second service system 206, a second verification system 208, and a first blockchain node 212 and a second blockchain node 214 on a blockchain network 210.

[0053] The first service system 202 is configured to send first service data to the first verification system, and the first service data includes, for a piece of data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data.

[0054] The first verification system 204 is configured to: collect the first service data of the first service system based on a predetermined condition and generate a first verification file including the first service data.

[0055] The second service system 206 is configured to send second service data to the second verification system, and the second service data includes, for a piece of data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data.

[0056] The second verification system 208 is configured to: receive the second service data of the second service system, determine a verification rule corresponding to the second service data based on the second service data, determine a mapping relationship between the second service data and the verification rule, and store the mapping relationship between the second service data and the verification rule in a local database.

[0057] The first verification system 204 is further configured to send a verification request to the second verification system, and the verification request includes the first verification file.

[0058] In some implementations of the present specification, the first verification system is further configured to: obtain the first service data, store N pieces of the first service data as the first verification file in response to a number of pieces of the first service data reaching a predetermined threshold N and process the first verification file to generate a first digital digest, and send the verification request to the second

verification system, the verification request including the first verification file and the first digital digest corresponding to the first verification file.

[0059] The second verification system 208 is configured to: receive the verification request, verify the first service data in the first verification file with the second service data in the local database and generate a verification result notification, send the verification result notification to the first verification system, and send successfully verified second service data in the local database to the first blockchain node on the blockchain network 210.

[0060] In some implementations of the present specification, the second verification system is further configured to: receive the verification request, extract the first digital digest from the verification request, and validate the first service data in the first verification file based on the first digital digest; and in response to the validating the first service data succeeding, determine the second service data corresponding to the first service data based on the identification information in the first service data, obtain the verification rule corresponding to the critical service information in the second service data, verify the first service data with the second service data in the local database based on the verification rule and generate the verification result notification, and send the verification result notification to the first verification system.

[0061] In some implementations of the present specification, the second verification system is further configured to: verify the first service data with the second service data in the local database based on the verification rule, generate a second verification file based on a result of the verifying the first service data with the second service data and process the second verification file to generate a second digital digest, and send the verification result notification to the first verification system, the verification result notification including the second verification file and the second digital digest corresponding to the second verification file.

[0062] The first verification system 204 is further configured to: receive the verification result notification, and send successfully verified first service data to the second blockchain node 214 on the blockchain network.

[0063] In some implementations of the present specification, the first verification system is further configured to: if unsuccessfully verified first service data exists in the second verification file, update the verification status of the unsuccessfully verified first service data and review or report the unsuccessfully verified first service data.

[0064] The first blockchain node 212 corresponds to a node of the blockchain network 210 and is configured to receive and store the successfully verified second service data that is sent by the second verification system.

[0065] The second blockchain node 214 corresponds to a node of the blockchain network 210 and is configured to receive and store the successfully verified first service data that is sent by the first verification system.

[0066] In some implementations of the present specification, the first blockchain node 212 and the second blockchain node 214 are further configured to: transmit successfully verified service data to other blockchain nodes, for the blockchain nodes of the blockchain network to reach a consensus on the successfully verified service data.

[0067] In some implementations of the present specification, real-time performance of service data verification is ensured by sending transaction service data of the service systems to the verification systems for subsequent data verification. Thereby, efficiency of the service data verification can be improved, and unsuccessfully verified data can be reviewed in time, which effectively ensures accuracy of the data.

[0068] FIG. 3 is a structural block diagram illustrating a computing device 300 according to some implementations of the present specification. Components of the computing device 300 include, but are not limited to, a memory 310 and a processor 320. The processor 320 is connected to the memory 310 through a bus 330, and a database 350 is configured to store data.

[0069] The computing device 300 further includes an access device 340, and the access device 340 enables the computing device 300 to communicate through one or more networks 360. Examples of these networks include a public switched telephone network (PSTN), a local area network (LAN), a wide area network (WAN), a personal area network (PAN), or a combination of communication networks such as the Internet. The access device 340 can include one or more of any types of wired or wireless network interfaces (for example, a network interface card (NIC)), such as an IEEE802.11 wireless local area network (WLAN) wireless interface, a worldwide interoperability for microwave access (Wi-MAX) interface, an Ethernet interface, a universal serial bus (USB) interface, a cellular network interface, a Bluetooth interface, a near field communication (NFC) interface, or the like.

[0070] In some implementations of the present specification, the above-described components of the computing device 300 and other components not shown in FIG. 3

can alternatively be connected to each other, for example, through a bus. It should be understood that the structural block diagram of the computing device shown in FIG. 3 is for an illustrative purpose only and is not intended to limit the scope of the present specification. A person skilled in the art can add or replace other components as required.

[0071] The computing device 300 can be any type of stationary or mobile computing device, including a mobile computer or a mobile computing device (for example, a tablet computer, a personal digital assistant, a laptop computer, a notebook computer, a netbook, or the like), a mobile phone (for example, a smartphone), a wearable computing device (for example, a smart watch, smart glasses, or the like), or another type of mobile device, or a stationary computing device such as a desktop computer or a PC. The computing device 300 can alternatively be a mobile or stationary server.

[0072] The processor 320 can perform steps in a blockchain-based data verification method shown in FIG. 4. FIG. 4 is a flowchart illustrating a blockchain-based data verification method according to some implementations of the present specification. The method includes step 402 to step 406.

[0073] Step 402: Collect first service data based on a predetermined condition and generate a first verification file including the first service data, the first service data including, for a piece of data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data.

[0074] In some implementations of the present specification, the predetermined condition is a predetermined number of pieces of transaction data. In practice, the predetermined condition can alternatively be specific predetermined duration, which is not limited in the present application.

[0075] In some implementations of the present specification, a predetermined threshold N is a positive integer, and a size of N can be determined based on an actual situation.

[0076] The first service data can further include transaction time and a transaction amount. For example, the predetermined threshold N is equal to 3. Assuming that the first service data is service data generated by an Internet insurance sales platform transaction, and first service data collected by a first verification system is listed in the form of a table, the first verification file is shown in Table 1:

Table 1

Identification information	Transaction time	Transaction amount	Critical service information	Verification status
User B - Platform A	02/03/2019 13:23	5,000 yuan	User B purchases a personal accident insurance with a policy number of A00001 on platform A.	Unverified
User C - Platform A	02/10/2019 09:15	3,600 yuan	User C purchases a vehicle insurance with a policy number of C00101 on platform A.	Unverified
User D - Platform A	02/10/2019 15:08	4,000 yuan	User D purchases a health insurance with a policy number of D10001 on platform A.	Unverified

[0077] Information in Table 1 includes: transaction identification information, the transaction time, the transaction amount, critical information of transaction, and a verification status of transaction data. After the first verification file is generated, the first verification file is processed to obtain a first digital digest, and the first verification file and the first digital digest are sent to a second verification system for data verification.

[0078] Step 404: Send a verification request to the second verification system, the verification request including the first verification file.

[0079] In some implementations of the present specification, the verification request further includes the first digital digest corresponding to the first verification file. After receiving the verification request, the second verification system can validate the first verification file based on the first digital digest to ensure that the first verification file is not tampered with. In response to the validating the first verification file succeeding, second service data corresponding to the first service data is searched for based on the identification information of the first service data, the first service data in the first verification file is verified based on a verification rule of the second service data, and a second verification file is generated based on a verification result.

[0080] Step 406: Receive a verification result notification sent by the second verification system, and send successfully verified first service data to a second blockchain node.

[0081] In some implementations of the present specification, the second verification system generates the second verification file based on the verification result, processes the second verification file to generate a second digital digest, and sends the second verification file and the second digital digest to the first verification system. The first verification system can validate the second verification file based on the second digital digest to ensure that the second verification file is not tampered with.

[0082] If all of the first service data in the first verification file is successfully verified, the second verification file generated based on the verification result is shown in Table 2:

Table 2

Identification information	Transaction time	Transaction amount	Critical information	Verification status
User B - Institution A	02/03/2019 13:23	5,000 yuan	User B purchases a personal accident insurance with a policy number of A00001 on platform A.	Successfully verified
User C - Institution A	02/10/2019 09:15	3,600 yuan	User C purchases a vehicle insurance with a policy number of C00101 on platform A.	Successfully verified
User D - Institution A	02/10/2019 15:08	4,000 yuan	User D purchases a health insurance with a policy number of D10001 on platform A.	Successfully verified

[0083] In some implementations of the present specification, if all of the first service data in the first verification file is successfully verified, the second verification file is shown in Table 2, and only the verification status is changed on the basis of Table 1.

[0084] If the first service data in the first verification file includes unsuccessfully verified service data, the second verification file is shown in Table 2.

[0085] In some implementations of the present specification, if the first verification file includes unsuccessfully verified service data, the second verification file is shown in Table 3.

Table 3

Identification information	Verification status	Verification failure cause
User B - Institution A	Successfully verified	None
User C - Institution A	Successfully verified	None
User D - Institution A	Unsuccessfully verified	No matching transaction service data is identified

[0086] Information in the second verification file includes: the identification information, a validation result, and the verification failure cause. The first verification system updates the verification status of the unsuccessfully verified service data, and reviews or reports the unsuccessfully verified service data.

[0087] In some implementations of the present specification, setting a reasonable service data number threshold in the first verification system not only can ensure real-time verification of the service data, but also can avoid pressure on the service systems caused by excessive service data to be verified, thereby effectively improving working efficiency.

[0088] FIG. 5 shows a blockchain-based data verification method according to some implementations of the present specification. The method includes step 502 to step 508.

[0089] Step 502: Obtain second service data of a second service system and store the second service data in a local database.

[0090] In some implementations of the present specification, the second service data is transaction service data generated by the second service system. The second service data includes, for a piece of transaction service data, identification information of the piece of transaction service data, critical service information of the piece of transaction service data, and a verification status of the piece of transaction service data, and can further include information such as transaction time and a transaction amount.

[0091] In some implementations of the present specification, after obtaining the second service data, a second verification system needs to determine a verification rule corresponding to the second service data based on the second service data, determine a mapping relationship between the second service data and the verification rule, and store the mapping relationship between the second service data and the verification rule in the local database.

[0092] An insurance service is still used as an example, the second service data obtained by the second service system is still listed in the form of a table, and it is assumed that the obtained second service data is shown in Table 4:

Table 4

Identification information	Transaction time	Transaction amount	Critical information	Verification status
Institution A - User B	02/03/2019 13:23	5,000 yuan	Institution A sells a personal accident insurance with a policy number of A00001 to user B.	Unverified

[0093] Information that can be obtained from Table 4 is: on February 03, 2019, institution A sold a personal accident insurance to user B, the policy number is A00001, the transaction amount is 5,000 yuan, and this piece of transaction information had not been verified. A verification rule for this piece of transaction information determined by the second verification system based on content of this piece of transaction information is as follows: the transaction time, the transaction amount and the verification status need to be consistent with those in Table 4, and the identification information and the critical information need to correspond to those in Table 4.

[0094] Step 504: Receive a verification request, the verification request including a first verification file.

[0095] In some implementations of the present specification, N pieces of first service data are stored as the first verification file in response to a number of pieces of the first service data obtained by a first verification system reaching a predetermined threshold N, and the first verification file is processed to generate a first digital digest, and the first verification file and the first digital digest are sent to the second verification

system. The second verification system can validate the first verification file based on the first digital digest to ensure that the first verification file is not tampered with.

[0096] Step 506: Verify the first service data in the first verification file with the second service data in the local database and generate a verification result notification, and send the verification result notification to the first verification system.

[0097] In some implementations of the present specification, after receiving the verification request and successfully validating the first verification file, the second verification system determines the corresponding second service data based on identification information of the first service data in the first verification file, and verifies the first service data based on the verification rule corresponding to the second service data. If information about the first service data complies with the above-described verification rule, the verification succeeds; if at least one piece of information of the first service data does not comply with the above-described verification rule, the verification fails.

[0098] A second verification file is generated based on a verification result, the second verification file is processed to generate a second digital digest, and the second verification file and the second digital digest are sent to the first verification system. The first verification system can validate the second verification file based on the second digital digest to ensure that the second verification file is not tampered with.

[0100] Step 508: Send successfully verified second service data in the local database to a first blockchain node on a blockchain network.

[0101] In some implementations of the present specification, after receiving successfully verified service data, the first blockchain node and a second blockchain node transmit the successfully verified service data to other blockchain nodes, for the blockchain nodes of the blockchain network to reach a consensus on successfully verified first service data.

[0102] FIG. 6 is a schematic interactive diagram illustrating a blockchain-based data verification method according to some implementations of the present specification. The method includes step 602 to step 616.

[0103] Step 602: A first verification system receives first service data from a first service system.

[0104] Step 604: A second verification system receives second service data from a second service system.

[0105] In some implementations of the present specification, the first service data and the second service data each include, for a piece of data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data, and further include transaction time and a transaction amount.

[0106] Step 606: The first verification system collects the first service data based on a predetermined condition and generates a first verification file including the first service data.

[0107] In some implementations of the present specification, the predetermined condition is a predetermined number of pieces of transaction data. A predetermined number threshold N is a positive integer, and a size of N can be determined based on an actual situation.

[0108] N pieces of the first service data are stored as the first verification file in response to the number of pieces of the first service data obtained by the first verification system reaching a predetermined threshold N, and the first verification file is processed to generate a first digital digest, and the first verification file and the first digital digest are sent to the second verification system. The second verification system can validate the first verification file based on the first digital digest to ensure that the first verification file is not tampered with.

[0109] Step 608: The first verification system sends a verification request to the second verification system.

[0110] In some implementations of the present specification, the verification request further includes the first digital digest corresponding to the first verification file. After receiving the verification request, the second verification system can validate the first verification file based on the first digital digest. In response to the validating the first verification file succeeding, the second service data corresponding to the first service data is searched for based on the identification information of the first service data, the first service data in the first verification file is verified based on a verification rule for the second service data, and a second verification file is generated based on a verification result.

[0111] Step 610: The second verification system verifies the first service data.

[0112] In some implementations of the present specification, after obtaining the second service data, the second verification system needs to determine the verification rule corresponding to the second service data based on the second service data,

determine a mapping relationship between the second service data and the verification rule, and store the mapping relationship between the second service data and the verification rule in a local database.

[0113] In some implementations of the present specification, after receiving the verification request and successfully validating the first verification file, the second verification system determines the corresponding second service data based on the identification information of the first service data in the first verification file, and verifies the first service data based on the verification rule corresponding to the second service data. If information of the first service data complies with the above-described verification rule, the verification succeeds; if at least one piece of information of the first service data does not comply with the above-described verification rule, the verification fails.

[0114] The second verification file is generated based on a verification result, the second verification file is processed to generate a second digital digest, and the second verification file and the second digital digest are sent to the first verification system. The first verification system can validate the second verification file based on the second digital digest to ensure that the second verification file is not tampered with.

[0115] Step 612: The second verification system sends a verification result notification to the first verification system.

[0116] In some implementations of the present specification, the second verification system generates the second verification file based on the verification result, processes the second verification file to generate a second digital digest, and sends the second verification file and the second digital digest to the first verification system. The first verification system can validate the second verification file based on the second digital digest to ensure that the second verification file is not tampered with.

[0117] Step 614: The first verification system sends successfully verified first service data to a second blockchain node.

[0118] Step 616: The second verification system sends successfully verified second service data to a first blockchain node.

[0119] In some implementations of the present specification, after receiving successfully verified service data, the first blockchain node and the second blockchain node transmit the successfully verified service data to other blockchain nodes, for the

blockchain nodes of the blockchain network to reach a consensus on the successfully verified first service data.

[0120] In some implementations of the present specification, the verification systems are established outside the service systems. Without affecting normal interaction between the service systems, data verification is completed through interaction between the verification systems, which improves efficiency of data verification and timeliness. In addition, the verified transaction service data is uploaded to a blockchain of a blockchain network, which ensures immutability and credibility of the data.

[0121] Some implementations of the present specification further provide a computing device, including: a memory, a processor, and a computer instruction stored in the memory and executable on the processor, where the steps of the blockchain-based data verification method are implemented when the processor executes the instruction.

[0122] Some implementations of the present application further provide a computer-readable storage medium, where the computer-readable storage medium stores a computer instruction, and the steps of the above-described blockchain-based data verification method are implemented when the instruction is executed by a processor.

[0123] The schematic solution for the computer-readable storage medium in these implementations has been described above. It should be noted that the technical solution of the storage medium belongs to the same concept as the technical solution of the above-described blockchain-based data verification method. For details that are not described in detail in the technical solution of the storage medium, references can be made to the description of the technical solution of the above-described blockchain-based data verification method.

[0124] Specific implementations of the present specification have been described above. Other implementations fall within the scope of the appended claims. In some situations, the actions or steps described in the claims can be performed in an order different from the order in the implementations and the desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily require a particular execution order to achieve the desired results. In some implementations, multi-tasking and parallel processing can be advantageous.

[0125] The computer instruction includes computer program code, which can be in a source code form, an object code form, an executable file or a certain intermediate form, or the like. The computer-readable medium can include any entity or device capable of including the computer program code, a recording medium, a USB flash drive, a removable hard disk, a magnetic disk, an optical disc, a computer memory, a read-only memory (ROM), a random access memory (RAM), an electrical carrier signal, a telecommunications signal, a software distribution medium, or the like. It should be noted that the content contained in the computer-readable medium can be appropriately increased or decreased in accordance with the requirements of the legislation and patent practice in the jurisdiction, for example, in some jurisdictions, the computer-readable medium does not include electrical carrier signals and telecommunications signals in accordance with the legislation and patent practice.

[0126] It should be noted that, for the sake of simplicity of description, the above-described method implementations are described as a series of action combinations, but a person skilled in the art should appreciate that the present application is not limited by the described action order, because some steps can be performed in other orders or at the same time according to the present application. In addition, a person skilled in the art should also appreciate that the implementations described in the present specification are example implementations and that the actions and modules involved are not necessarily required by the present application.

[0127] In the above-described implementations, the descriptions of the implementations have respective focuses. For a part that is not described in detail in some implementations, references can be made to related descriptions in other implementations.

[0128] The example implementations of the present application disclosed above are intended only to aid in the elaboration of the present application. The optional implementations do not describe all the details in detail, nor do they limit the present invention to the specific implementations described. Clearly, many modifications and changes can be made according to the content of the present specification. These implementations are selected and described in detail in the present specification in order to better explain the principles and practical applications of the present application, so that a person skilled in the art can well understand and use the present application. The present application is limited only by the claims and their full scope and equivalents.

CLAIMS

What is claimed is:

1. A computer-implemented method performed by a blockchain-based data verification system, wherein the blockchain-based data verification system comprises a first verification system, a second verification system, a first blockchain node and a second blockchain node on a blockchain network, the method comprising:

collecting, by the first verification system, first service data based on a predetermined condition, wherein the first service data comprises pieces of transaction service data of a first service system and the predetermined condition is the obtaining, by the first verification system and from the first service system, of a number of pieces of transaction service data of the first service system that reaches a predetermined threshold N, wherein N is a positive integer;

generating, by the first verification system, a first verification file including the first service data;

processing, by the first verification system, the first verification file to generate a first digital digest;

sending, by the first verification system, a verification request to the second verification system, the verification request including the first verification file and the first digital digest;

receiving, by the second verification system, second service data from a second service system, wherein the second service data is transaction service data of the second service system, and storing the second service data in a local database of the second verification system;

receiving, by the second verification system, the verification request from the first verification system;

extracting, by the second verification system, the first digital digest from the verification request;

validating, by the second verification system, the first service data in the first verification file based on the first digital digest;

in response to that the validating the first service data succeeds, determining, by the second verification system, the second service data corresponding to the first service data based on identification information in the first service data;

obtaining, by the second verification system, a verification rule for the second service data, the verification rule corresponding to critical service information in the second service data;

verifying, by the second verification system, the first service data with the second service data based on the verification rule;

generating, by the second verification system, a verification result notification;

sending, by the second verification system, the verification result notification to the first verification system;

receiving, by the first verification system, the verification result notification;

sending, by the first verification system, successfully verified first service data to the second blockchain node on the blockchain network;

sending, by the second verification system, successfully verified second service data in the local database to the first blockchain node on the blockchain network;

after receiving and storing, by the second blockchain node, the successfully verified first service data that is sent by the first verification system and receiving and storing, by the first blockchain node, the successfully verified second service data that is sent by the second verification system, transmitting, by the second blockchain node and the first blockchain node, the successfully verified first service data and the successfully verified second service data to other blockchain nodes for the blockchain nodes of the blockchain network to reach a consensus on the successfully verified first service data and the successfully verified second service data and store the successfully verified first service data and the successfully verified second service data in a blockchain of the blockchain network.

2. The method according to claim 1, wherein the first service data includes, for a piece of data of the first service data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data; and

wherein the second service data includes, for a piece of data of the second service data, identification information of the piece of data, critical service information of the piece of data, and a verification status of the piece of data.

3. The method according to claim 2, wherein the first service data is sent by the first service system to the first verification system and the second service data is sent by the second service system to the second verification system.

4. The method according to claim 1, comprising the following steps performed by the first verification system:

obtaining pieces of transaction service data of the first service system; and

storing the obtained pieces of transaction service data of the first service system as the first verification file in response to that the number of the obtained pieces of transaction service data of the first service system reaches the predetermined threshold N.

5.The method according to claim 1, further comprising the following steps performed by the second verification system:

generating a second verification file based on a result of the verifying the first service data with the second service data;

processing the second verification file to generate a second digital digest; and

sending the verification result notification to the first verification system, the verification result notification including the second verification file and the second digital digest corresponding to the second verification file.

6. A blockchain-based data verification system comprising a first verification system, a second verification system, a first blockchain node and a second blockchain node on a blockchain network, wherein the blockchain-based data verification system is configured to carry out the steps of the method according to any one of claims 1 to 5.