

INFORMATION PROCESSING METHOD AND DEVICE BASED ON BLOCKCHAIN, AND COMPUTER-READABLE STORAGE MEDIUM

RELATED APPLICATION

5 **[0001]** This application claims priority to Chinese Patent Application No. 201910319332.9, titled "BLOCKCHAIN-BASED INFORMATION PROCESSING METHOD AND APPARATUS AND COMPUTER-READABLE STORAGE MEDIUM" and filed with the China National Intellectual Property Administration on April 19, 2019, which is incorporated herein by reference in its entirety.

FIELD OF THE TECHNOLOGY

10 **[0002]** This application relates to the field of computer technologies, and in particular, to a blockchain-based information processing method and apparatus and a computer-readable storage medium.

BACKGROUND OF THE DISCLOSURE

15 **[0003]** With the development of computer technologies, blockchain data processing technology keeps developing. The blockchain technology (BT) is also referred to as distributed ledger technology and is an Internet database technology that features decentralization, openness, and transparency, enabling all people to participate in database recording. Currently, blockchains mainly include public blockchain, private blockchain, consortium blockchain, permissioned
20 blockchain, and hybrid blockchain.

[0004] The security of transaction information needs to be considered for BT-based transactions. A currently adopted solution is implemented based on a plaintext sensitive vocabulary. Specifically, a service provider maintains a plaintext sensitive vocabulary. When a user needs to detect and filter content, original content is transmitted to a server. The server uses the plaintext
25 sensitive vocabulary to compare and filter the original content provided by the user, and then returns a result to a client. After receiving the filtered content and a detection result, the client may perform subsequent processing.

[0005] However, the currently adopted sensitive vocabulary is maintained in a centralized organization in the form of plaintext. When the sensitive vocabulary needs to be updated, a plaintext

sensitive vocabulary file is usually used for synchronizing with latest sensitive words. Therefore, if a carrier file of the sensitive vocabulary leaks during synchronization, potential security hazards may arise in transaction information, causing a series of harms to society.

SUMMARY

5 **[0006]** Embodiments of this application provide a blockchain-based information processing method and apparatus and a computer-readable storage medium. A record of index information is no longer maintained in the form of plaintext, but an index of the index information involved during a blockchain transaction is recorded, thereby forming variant index information. The variant index information does not directly display specific content of the index information, but is maintained in
10 the form of the index, so that potential security hazards are less likely to arise, and the security of information maintenance is improved.

[0007] An aspect of this application provides a blockchain-based information processing method, performed by a network node device, and including:

obtaining an original index information set, the original index information set
15 including at least one piece of original index information, each piece of original index information including plaintext sensitive content;

obtaining information in to-be-matched blocks, the information including
information content and an information index, the information content having a correspondence
with the information index;

20 matching the information content in the information by using the original index information set, to obtain a matching result; and

generating a variant index information set according to the matching result in a case
that the matching result indicates that the matching succeeds, the variant index information set
including at least one piece of variant index information, the variant index information including the
25 information index corresponding to the information content in the information.

[0008] An aspect of this application provides a blockchain-based information processing method, performed by a network node device, and including:

receiving request information, the request information carrying a to-be-detected
information index;

30 detecting, by using a variant index information set, the to-be-detected information index carried by the request information, to obtain a detection result, the variant index information

set including at least one piece of variant index information, the variant index information including an information index in information;

obtaining information content corresponding to the to-be-detected information index;

5 processing the information content corresponding to the to-be-detected information index according to the detection result, to obtain processed information; and

transmitting the processed information, to display the processed information.

[0009] An aspect of this application provides a blockchain-based data processing apparatus, including:

10 an obtaining module, configured to obtain an original index information set, the original index information set including at least one piece of original index information, each piece of original index information including plaintext sensitive content,

the obtaining module being further configured to obtain information in to-be-matched blocks, the information including information content and an information index, the information content having a correspondence with the information index;

15 a matching module, configured to match the information content in the information by using the original index information set obtained by the obtaining module, to obtain a matching result; and

a generation module, configured to generate a variant index information set according to the matching result in a case that the matching result obtained by the matching module indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index information including the information index corresponding to the information content in the information.

[0010] In a possible design, the matching module is configured to: match first information content by using the original index information set, the first information content belonging to the information; and

25 match information content in a second block in a case that the first information content is the last piece of information in a first block, the first block being a block of the to-be-matched blocks, the second block being another block of the to-be-matched blocks, the second block being a next block adjacent to the first block; or

30 obtain second information content in the first block in a case that the first information content is not the last piece of information in the first block, and match the second

information content by using the original index information set, the second information content being a next piece of information content adjacent to the first information content.

[0011] In a possible design, the generation module is configured to: obtain a sensitivity level of the original index information in a case that the matching result is that the information
5 successfully matches the original index information in the original index information set;

obtain a hash value, an intra-block index, and a block height in the information index, the intra-block index representing a position of the information in the to-be-matched block; and

generate the variant index information set according to the sensitivity level of the original index information, the hash value, the intra-block index, and the block height.

10 **[0012]** In a possible design, the blockchain-based data processing apparatus further includes a processing module, where

the processing module is configured to: receive request information after the generation module generates a variant index information set according to the matching result, the request information carrying a to-be-detected information index;

15 detect the to-be-detected information index by using the variant index information set, to obtain a detection result; and

process the request information according to the detection result.

[0013] In a possible design, the processing module is configured to: determine a target hash value according to the to-be-detected information index;

20 match the target hash value by using the variant index information set;

determine, in a case that the target hash value successfully matches the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive information; and

25 determine, in a case that the target hash value fails to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

[0014] In a possible design, the processing module is configured to: determine a target intra-block index and a target block height according to the to-be-detected information index;

30 match the target intra-block index and the target block height by using the variant index information set;

determine, in a case that the target intra-block index and the target block height successfully match the variant index information in the variant index information set, that the to-be-detected information index is sensitive transaction information; and

5 determine, in a case that the target intra-block index and the target block height fail to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

[0015] In a possible design, the processing module is configured to: obtain target information content according to the to-be-detected information index in a case that information content corresponding to the to-be-detected information index is secure information; and

10 transmit the target information content to a client, to enable the client to display the target information content.

[0016] In a possible design, the processing module is configured to: determine a target sensitivity level and a target service type according to the to-be-detected information index in a case that the information content corresponding to the to-be-detected information index is sensitive
15 information;

determine, according to the target sensitivity level and the target service type, whether to display the target information content corresponding to the to-be-detected information index;

20 transmit prompt information to the client in a case of determining not to display the target information content, to enable the client to display the prompt information, the prompt information being used for prompting a user that the target information content is the sensitive information; and

process the target information content in a case of determining to display the target information content to obtain processed target information content, and transmit the processed
25 target information content to the client, to enable the client to display the processed target information content.

[0017] In a possible design, the processing module is configured to: obtain the target information content;

30 match the target information content by using the original index information set, and determine target index information in the target information content; and

block the target index information in the target information content, to obtain the

processed target information content.

[0018] An aspect of this application provides a blockchain-based data processing apparatus, including:

a receiving module, configured to receive request information, the request

5 information carrying a to-be-detected information index;

a detection module, configured to detect, by using a variant index information set, the to-be-detected information index carried by the request information, to obtain a detection result, the variant index information set including at least one piece of variant index information, the variant index information including an information index in information;

10 an obtaining module, configured to obtain information content corresponding to the to-be-detected information index;

a processing module, configured to process the information content corresponding to the to-be-detected information index according to the detection result, to obtain processed information; and

15 a transmission module, configured to transmit the processed information, to display the processed information.

[0019] An aspect of this application provides a network node device, including a memory and a processor,

the memory being configured to store a program;

20 the processor being configured to execute the program in the memory, to perform the following operations:

obtaining an original index information set, the original index information set including at least one piece of original index information, each piece of original index information including plaintext sensitive content;

25 obtaining information in to-be-matched blocks, the information including information content and an information index, the information content having a correspondence with the information index;

matching the information content in the information by using the original index information set, to obtain a matching result; and

30 generating a variant index information set according to the matching result in a case

that the matching result indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index information including the information index corresponding to the information content in the information.

[0020] An aspect of this application provides a network node device, including a memory and a processor,

the memory being configured to store a program;

the processor being configured to execute the program in the memory, to perform the following operations:

receiving request information, the request information carrying a to-be-detected information index;

detecting, by using a variant index information set, the to-be-detected information index carried by the request information, to obtain a detection result, the variant index information set including at least one piece of variant index information, the variant index information including an information index in information;

obtaining information content corresponding to the to-be-detected information index;

processing the information content corresponding to the to-be-detected information index according to the detection result, to obtain processed information; and

transmitting the processed information, to display the processed information.

[0021] According to an aspect of this application, a computer-readable storage medium storing instructions is provided, the instructions, when run on a computer, causing the computer to perform the foregoing methods.

[0022] According to the foregoing technical solutions, it can be learned that the embodiments of this application have the following advantages:

[0023] In the embodiments of this application, a blockchain-based information processing method is provided. First, an original index information set is obtained, the original index information set including at least one piece of original index information, each piece of original index information including plaintext sensitive content; information in to-be-matched blocks is then obtained, the information including information content and an information index, the information content having a correspondence with the information index; and the information content in the information is matched by using the original index information set, to obtain a matching result, and a variant index information set is generated according to the matching result in

a case that the matching result indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index information including the information index corresponding to the information content in the information. Through the foregoing methods, a record of index information is no longer maintained in the form of plaintext,
5 but an information index of the index information involved during a blockchain transaction is recorded, thereby forming variant index information. The variant index information does not directly display specific content of the index information, but is maintained in the form of the information index, so that potential security hazards are less likely to arise, and the security of information maintenance is improved.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] FIG. 1 is a schematic architectural diagram of a blockchain-based information processing system according to an embodiment of this application.

[0025] FIG. 2 is a schematic structural composition diagram of a block according to an embodiment of this application.

15 [0026] FIG. 3 is a schematic diagram of an embodiment of a blockchain-based information processing method according to an embodiment of this application.

[0027] FIG. 4 is a schematic flowchart of updating a variant index information set according to an embodiment of this application.

[0028] FIG. 5 is a schematic flowchart of applying a variant index information set according
20 to an embodiment of this application.

[0029] FIG. 6 is a schematic flowchart of applying a variant index information set according to an embodiment of this application.

[0030] FIG. 7 is a schematic diagram of a blockchain-based information processing method according to an embodiment of this application.

25 [0031] FIG. 8 is a schematic flowchart of displaying processed transaction information by a client according to an embodiment of this application.

[0032] FIG. 9 is a schematic diagram of a blockchain-based information processing apparatus according to an embodiment of this application.

[0033] FIG. 10 is a schematic diagram of a blockchain-based information processing
30 apparatus according to an embodiment of this application.

[0034] FIG. 11 is a schematic diagram of a blockchain-based information processing apparatus according to an embodiment of this application.

[0035] FIG. 12 is a schematic structural diagram of a network node device according to an embodiment of this application.

5

DESCRIPTION OF EMBODIMENTS

[0036] Embodiments of this application provide a blockchain-based information processing method and apparatus and a computer-readable storage medium. A record of index information is no longer maintained in the form of plaintext, but an index of the index information involved during a blockchain transaction is recorded, thereby forming variant index information. The variant index
10 information does not directly display specific content of the index information, but is maintained in the form of the index, so that potential security hazards are less likely to arise, and the security of information maintenance is improved.

[0037] In the specification, claims, and accompanying drawings of this application, the terms "first", "second", "third", "fourth", and so on (if any) are intended to distinguish between
15 similar objects rather than describe a specific order or sequence. It may be understood that the data termed in such a way is interchangeable in proper circumstances, so that the embodiments of this application described herein, for example, can be implemented in other orders than the order illustrated or described herein. In addition, the terms "include", "corresponding to" and any other
20 variants are intended to cover the non-exclusive inclusion. For example, a process, method, system, product, or device that includes a series of steps or units is not necessarily limited to those expressly listed steps or units, but may include other steps or units not expressly listed or inherent to such a process, method, product, or device.

[0038] It is to be understood that the information processing method provided by this application is applicable to a blockchain system. The blockchain is a bookkeeping technology in
25 which multiple parties carry out maintenance, transmission and access security is ensured by using cryptography, and consistent data storage, tamper resistance, and non-repudiation can be achieved. The technology is also referred to as distributed ledger technology. A typical blockchain stores data in a block-chain structure.

[0039] This application may be specifically applied to a public blockchain, a private
30 blockchain or a consortium blockchain. The public blockchain has no official organization, no management organization, and no central server. Participating nodes freely access a network according to a system rule and without any control, and the nodes work based on a consensus

mechanism. A private blockchain is established within a group. An operation rule of a system is set according to requirements of the group, and modification or read rights are restricted to some extent. Meanwhile, such features as authenticity and partial decentralization of the blockchain are preserved. A consortium blockchain is jointly initiated by several mechanisms and is a concept that
5 lies between a public blockchain and a private blockchain, and has a feature of partial decentralization. Read rights on the blockchain may be open to public or partially open to public. That is, a plurality of pre-selected nodes are internally appointed as bookkeepers. The bookkeepers contest for the bookkeeping right, and other access nodes may participate in transactions but do not interfere in a bookkeeping process.

10 **[0040]** For ease of understanding, this application provides a blockchain-based information processing method. The method is applicable to an information processing system shown in FIG. 1. FIG. 1 is a schematic architectural diagram of a blockchain-based information processing system according to an embodiment of this application. As shown in FIG. 1, the architecture of the information processing system may include distributed nodes (for example, a network node device
15 1, a network node device 2, a network node device 3, a network node device 4, a network node device 5, and a network node device 6). The distributed nodes are connected by a communication link. For example, the distributed nodes may be connected by a wired communication link or a wireless communication link. The plurality of distributed nodes jointly form a blockchain network. A quantity of the distributed nodes (six distributed nodes) shown in FIG. 1 is merely exemplary, and
20 any quantity of distributed nodes may be deployed according to an actual requirement.

[0041] In an embodiment of this application, the network node devices may generate transaction information according to update information of public configuration parameters (for example, a node quantity, a block size, and a block generation period) in the blockchain network. The transaction information is then broadcast in the blockchain network, so that the network node
25 devices in the blockchain network may verify and validate the transaction information. After the network node devices in the blockchain network reach a consensus on the transaction information, the public configuration parameters may be updated according to the transaction information, so that the public configuration parameters can be updated during the operation of the blockchain nodes, thereby improving the update efficiency of the public configuration parameters.

30 **[0042]** For any network node device in the foregoing blockchain, a user may initiate a transaction request to the network node device by using a client. The transaction request carries a to-be-detected information index. The network node device uses a variant index information set to detect the to-be-detected information index in the transaction request, to obtain a detection result. In

a case that the detection result shows that the to-be-detected information index does not have sensitive information, the network node device may obtain target information content corresponding to the transaction request from another network node device, and transmit the target information content to the client. The client displays the target information content in plaintext form. Otherwise,
5 in a case that the detection result shows that the to-be-detected information index has sensitive information, the target information content involving index information needs to be completely blocked or partially blocked. The client is deployed on a terminal device. The terminal device includes, but is not limited to, a tablet computer, a notebook computer, a palmtop computer, a mobile phone, and a personal computer (PC), which is not limited herein.

10 **[0043]** FIG. 2 is a schematic structural composition diagram of a block according to an embodiment of this application. As shown in FIG. 2, a blockchain is formed by a plurality of blocks. The blocks are data organization units in a blockchain network and are connected in series by a linked list. The block includes a block header and a block body. The block header includes a hash value of a preceding block, a timestamp of the current block, a block height, and other information.
15 The hash value of the preceding block is used for linking the block to the preceding block in the blockchain. The timestamp of the current block is used for determining the generation time of the block. The block height is used for representing a position of the block in the blockchain. Other information includes a Merkle root, a difficulty target, and a random value of the block body. The block body includes transaction information, for example, "A transfers 50 bitcoins to B". Each piece
20 of transaction information corresponds to a hash value. The hash value can uniquely and accurately identify a piece of transaction information, and each block maintains the same transaction information.

[0044] The following describes the blockchain-based information processing method in this application with reference to the foregoing description. The blockchain-based information
25 processing method may be performed by a computer device. The computer device may be the network node device in FIG. 1. Referring to FIG. 3, the blockchain-based information processing method according to an embodiment of this application includes the following steps 101 to 104.

[0045] Step 101 includes obtaining an original index information set, the original index information set including at least one piece of original index information, each piece of original
30 index information including plaintext sensitive content.

[0046] In this embodiment, an information processing apparatus in the network node device first needs to obtain an original index information set. The original index information set includes a word and phrase set related to information about pornography, violence, reaction, and fraud. The

original index information set may be specifically a vocabulary and represented in a table structure. Table 1 is an example of the original index information set.

Table 1

Column name	Data type	Description
ID	Int32	Unique ID of original index information
Sensitivity level	Int8	Sensitivity level: 1: Common sensitivity 2: Intermediate sensitivity 3: High sensitivity
Index information content	String	Original sensitive content, which may be a common word or a regular expression.

[0047] As shown in Table 1, one piece of original index information corresponds to a unique identification (ID). The original index information is usually a phrase, or may be a word or a sentence. The sensitivity level represents a sensitivity degree of the original index information. Original index information of different levels may be processed differently. The index information content is specifically a phrase or sentence, which may be represented in the form of common text or a regular expression. The data type corresponding to the ID is a signed 32-bit integer and occupies four bytes. The data type corresponding to the sensitivity level is a signed 8-bit integer and occupies one byte. The data type corresponding to the index information content is string. It may be understood that Table 1 is merely an example and shall not be construed as a limitation to the original index information set.

[0048] Step 102 includes obtaining information in to-be-matched blocks, the information including information content and an information index, the information content having a correspondence with the information index.

[0049] In this embodiment, the information processing apparatus obtains information in to-be-matched blocks. It is assumed that there are N blocks in a blockchain and the N blocks may be the to-be-matched blocks. Each block has corresponding information. The information specifically includes information content and an information index. The information content includes a user-defined field. The information index may include a hash value, an intra-block index, and a block height.

[0050] It may be understood that each block has a block height. The block height represents a position of the block in the blockchain, that is, a position with respect to a first block. The block height of the first block is defined to be 0. Based on this, subsequent block heights sequentially increase. The block height is not a unique identifier of the block, because the blockchain may
5 diverge, producing two or more blocks at the same height. That is, each block has a unique block height, but one block height does not correspond to a unique block. Each piece of information content in the block corresponds to a unique hash value. Each piece of information content has one intra-block index. Assuming that the blockchain is a ledger, where the block is a piece of paper in the ledger and each piece of information content is recorded in a line on the paper, the intra-block
10 index represents the line number and page number of the information content in the ledger.

[0051] Step 103 includes matching the information content in the information by using the original index information set, to obtain a matching result.

[0052] In this embodiment, the information processing apparatus matches each piece of information content in the information content against the original index information in the original
15 index information set, to obtain a matching result of each piece of information content. For example, information content 1 is "A recharges 50,000 Yuan RMB on behalf of B". The phrase "recharge on behalf of" is the original index information in the original index information set. Therefore, the matching result indicates that the matching succeeds. The information content 1 is a sensitive transaction. Information content 2 is "A transfers 100 Yuan RMB to C". The information does not
20 include the original index information in the original index information set. Therefore, the information content 2 is a secure transaction.

[0053] Step 104 includes generating a variant index information set according to the matching result in a case that the matching result indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index
25 information including the information index corresponding to the information content in the information.

[0054] In this embodiment, the information processing apparatus generates a variant index information set based on the matching result of the transaction information in a case that the matching result indicates that the matching succeeds, the variant index information set including at
30 least one piece of variant index information, the variant index information including information index in the information. Reference is made to Table 2, which is an example of the variant index information set.

Table 2

Column name	Data type	Description
Hash value	String	Hash value of a transaction where original index information is located
Sensitivity level	Int8	Sensitivity level: 1: Common sensitivity 2: Intermediate sensitivity 3: High sensitivity
Block height	Int64	Height of a block where original index information is located
Intra-block index	Int16	Index of original index information in the block

[0055] As shown in Table 2, the hash value represents a hash value corresponding to the original index information in information content. The sensitivity level represents a sensitivity degree of the original index information. Original index information of different levels may be processed differently. The block height represents a block height of a block where the original index information is located. The intra-block index represents information of the block where the original index information is located. The data type corresponding to the hash value is String. The data type corresponding to the sensitivity level is Int8. The data type corresponding to the block height is Int64. The data type corresponding to the intra-block index is Int16. It may be understood that Table 2 is merely an example and shall not be construed as a limitation to the variant index information set.

[0056] In the embodiments of this application, a blockchain-based information processing method is provided. First, an original index information set is obtained, the original index information set including at least one piece of original index information, each piece of original index information including plaintext sensitive content; information in to-be-matched blocks is then obtained, the information including information content and an information index, the information content having a correspondence with the information index; and the information content in the information is matched by using the original index information set, to obtain a matching result, and a variant index information set is generated according to the matching result in a case that the matching result indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index information including the information index corresponding to the information content in the information. Through the foregoing method, a

record of index information is no longer maintained in plaintext form, but an information index of the index information involved during a blockchain transaction is recorded, thereby forming variant index information. The variant index information does not directly display specific content of the index information, but is maintained in the form of the information index, so that potential security hazards are less likely to arise, and the security of information maintenance is improved.

[0057] Optionally, based on the embodiment corresponding to FIG. 3, in a blockchain-based information processing method according to an optional embodiment of this application, the matching the information content in the information by using the original index information set may include:

matching first information content by using the original index information set, the first information content belonging to the information; and

matching information content in a second block in a case that the first information content is the last piece of information in a first block, the first block being a block of the to-be-matched blocks, the second block being another block of the to-be-matched blocks, the second block being a next block adjacent to the first block; or

obtaining second information content in the first block in a case that the first information content is not the last piece of information in the first block, and matching the second information content by using the original index information set, the second information content being a next piece of information content adjacent to the first information content.

[0058] In this embodiment, a method for matching information content in transaction information by using the original index information set is described. Specifically, first, the first information content in the first block is matched. In a case that the first information content is the last piece of information in the first block, the first piece of information content in the second block is obtained for matching, the second block being a block next to the first block. In a case that the first information content is not the last piece of information in the first block, the second information content is obtained from the first block, and the second information content is matched by using the original index information set, until the matching of information content corresponding to each piece of information in each block is completed.

[0059] For ease of description, reference is made to FIG. 4, which is a schematic flowchart of updating a variant index information set according to an embodiment of this application. As shown in FIG. 4:

[0060] step S1 includes starting to match original index information;

[0061] step S2 includes initializing N to 1, and initializing X to 0, where N represents a block height and a block includes X pieces of information content,;

[0062] step S3 includes scanning an X^{th} piece of information content in the information content of a current block;

5 **[0063]** step S4 includes determining whether original index information exists in the X^{th} piece of information content, for example, whether a sensitive word exists, where step S5 is performed in a case that original index information exists, and step S6 is performed in a case that no original index information exists;

10 **[0064]** step S5 includes recording N and X in a case that original index information exists in the X^{th} piece of information content, where a hash value corresponding to the X^{th} piece of information content may further be recorded, that is, N is recorded in a block height field of the variant index information set, X is recorded in an intra-block index field, and the hash value is recorded in a hash value field;

15 **[0065]** step S6 includes continuing, in a case that no original index information exists in the X^{th} piece of information content, to determine whether the current block has a next piece of information content, where step S7 is performed in a case that the block has a next piece of information content, or step S8 is performed in a case that the block does not have a next piece of information content;

20 **[0066]** step S7 includes continuing to load the next piece of information content of the block in a case that the next piece of information content exists in the block with the height of N, that is, add 1 to X, that is, $X = X + 1$, where step S3 to step S6 are then performed again;

25 **[0067]** step S8 includes determining, in a case that no next piece of information content exists in the block with the height of N, whether there is a block corresponding to a next block height, that is, detecting whether there is a next N, where if a next N exists, step S10 is performed, or if no next N exists, step S9 is performed;

[0068] step S9 includes continuing to wait for the generation of a new block in a case that a block corresponding to the next block height does not exist; and

30 **[0069]** step S10 includes cyclically loading the block corresponding to the next block height in a case that the block corresponding to the next block height exists, and changing both N and X, that is, $N = N + 1$, and $X = 0$.

[0070] Thus, in the embodiment of this application, a method for matching transaction information by using an original index information set is provided. That is, the first information

content is matched by using the original index information set. The information content in the second block is matched in a case that the first information content is the last piece of transaction information in the first block, and in a case that the first information content is not the last piece of transaction information in the first block, the second information content in the first block is
5 obtained and matched by using the original index information set. Through the foregoing method, during actual matching, each piece of information content in each block is matched, to achieve a full scan of the block, thereby facilitating the generation of a more complete variant index information set.

[0071] Optionally, based on the embodiment corresponding to FIG. 3, in a blockchain-based
10 information processing method according to an optional embodiment of this application, the generating a variant index information set according to the matching result may include:

obtaining a sensitivity level of the original index information in a case that the matching result is that the information successfully matches the original index information in the original index information set;

15 obtaining a hash value, an intra-block index, and a block height in the information index, the intra-block index representing a position of the information in the to-be-matched block; and

generating the variant index information set according to the sensitivity level of the original index information, the hash value, the intra-block index, and the block height.

20 **[0072]** In this embodiment, representation forms of three types of variant index information sets are described. A sensitivity level of the original index information is obtained in a case that the matching result is that the information content in the information successfully matches the original index information in the original index information set. Specifically, one piece of information content is used as an example. Assuming that information content A matches a piece of original
25 index information A in the original index information set, the sensitivity level of the original index information A is obtained. In addition, a hash value and an intra-block index of the information content A may further be obtained. Assuming that the information content A belongs to a block M, a block height of the block M may then be obtained. According to the foregoing information, reference is made to Table 3, which is an example of the variant index information set.

Table 3

Column name	Data type	Description
Hash value	String	Hash value of a transaction where original index information is located
Sensitivity level	Int8	Sensitivity level: 1: Common sensitivity 2: Intermediate sensitivity 3: High sensitivity
Block height	Int64	Height of a block where original index information is located
Intra-block index	Int16	Index of original index information in the block

[0073] As can be seen in Table 3, the variant index information set may include the sensitivity level of the original index information, the hash value, the intra-block index, and the block height.

5 **[0074]** Table 4 is another example of the variant index information set.

Table 4

Column name	Data type	Description
Hash value	String	Hash value of a transaction where original index information is located
Sensitivity level	Int8	Sensitivity level: 1: Common sensitivity 2: Intermediate sensitivity 3: High sensitivity

[0075] As can be seen in Table 4, the variant index information set may include the sensitivity level of the original index information and the hash value.

[0076] Table 5 is another example of the variant index information set.

Table 5

Column name	Data type	Description
-------------	-----------	-------------

Sensitivity level	Int8	Sensitivity level: 1: Common sensitivity 2: Intermediate sensitivity 3: High sensitivity
Block height	Int64	Height of a block where original index information is located
Intra-block index	Int16	Index of original index information in the block

[0077] As can be seen in Table 5, the variant index information set may include the sensitivity level of the original index information, the intra-block index, and the block height, and the variant index information set is generated.

5 **[0078]** Thus, in the embodiment of this application, a manner of generating a variant index information set is provided. The sensitivity level of the original index information is obtained in a case that the matching result is that the information content successfully matches the original index information in the original index information set, and the hash value, the intra-block index, and the block height in the information index may then be obtained. The intra-block index represents a
10 position of the information content in the to-be-matched block. Finally, the variant index information set may be generated according to the sensitivity level of the original index information, the hash value, the intra-block index, and the block height. Alternatively, the variant index information set may be generated according to the sensitivity level of the original index information and the hash value. Alternatively, the variant index information set may be generated according to
15 the sensitivity level of the original index information, the intra-block index, and the block height. In the foregoing manner, the generated variant index information set may include different information. Three types of usable variant index information sets are listed herein, and information matching may be performed according to an actual requirement, thereby improving the flexibility and applicability of the solution.

20 **[0079]** Optionally, based on the embodiment corresponding to FIG. 3, in a third optional embodiment of this application, after the generating the variant index information set according to the matching result, the blockchain-based information processing method further includes:

receiving request information, the request information carrying a to-be-detected information index;

detecting the to-be-detected information index by using the variant index information set, to obtain a detection result; and

processing the request information according to the detection result.

[0080] In this embodiment, an application method of the variant index information set is described. When a user requests to display information, the request information may be transmitted by using a client, and the information processing apparatus receives the request information. The request information carries the to-be-detected information index, and the to-be-detected information index belongs to an original request. The information processing apparatus detects the to-be-detected information index and the variant index information in the variant index information set, to obtain the detection result. Finally, a processing manner of the request information is selected according to the detection result.

[0081] Thus, in the embodiment of this application, an application method of a variant index information set is provided. After the variant index information set is generated, the request information transmitted by the client may further be received, the to-be-detected information index is then detected by using the variant index information set to obtain the detection result, and finally, the request information is processed according to the detection result. In the foregoing manner, the information index is detected by using the variant index information set, so that the risk brought to a blockchain application by security supervision on blockchain content can be effectively resolved, so that the information index can be transmitted to providers of blockchain services while avoiding potential security hazards brought by direct transmission of original index information.

[0082] Optionally, based on the embodiment corresponding to FIG. 3, in a blockchain-based information processing method according to an optional embodiment of this application, the detecting the to-be-detected information index by using the variant index information set, to obtain a detection result, includes:

determining a target hash value according to the to-be-detected information index;

matching the target hash value by using the variant index information set;

determining, in a case that the target hash value successfully matches the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive information; and

determining, in a case that the target hash value fails to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

[0083] In this embodiment, a manner of detecting the to-be-detected information index is described. For ease of description, the description is made with reference to FIG. 5 below. FIG. 5 is a schematic flowchart of applying a variant index information set according to an embodiment of this application, which specifically includes:

5 **[0084]** step A1: first obtaining request information initiated by a user, determining a corresponding to-be-detected information index according to the request information, and obtaining a corresponding target hash value according to the to-be-detected information index;

[0085] step A2: obtaining an updated variant index information set, where because the quantity of blocks is subject to change, the variant index information set is usually updated in real
10 time;

[0086] step A3: matching the target hash value by using the variant index information set, that is, determining whether the target hash value hits a hash value in the variant index information set, where the process proceeds to step A4 in a case that the matching fails, or the process proceeds to step A7 in a case that the matching succeeds;

15 **[0087]** step A4: determining, in a case that the target hash value fails to match the variant index information in the variant index information set, that the to-be-detected information index is secure information, where in this case, target information content corresponding to the target hash value may be obtained from another block;

[0088] step A5: decoding the target information content, where the target information
20 content may be data serialized in the form of a bit group, and after the target information content is decoded, structural data readable by naked eyes may be obtained, that is, plaintext target information content is obtained;

[0089] step A6: feeding back the plaintext target information content to a client, for display of the client ;

25 **[0090]** step A7: determining, in a case that the target hash value successfully matches the variant index information in the variant index information set, that the to-be-detected information index is sensitive information, where in this case, it needs to be determined, according to a service requirement, whether the display of the target information content needs to be completely blocked, where step A11 is performed in a case that the target information content needs to be completely
30 blocked, or step A8 is performed in a case that the target information content does not need to be completely blocked;

[0091] step A8: obtaining the target information content corresponding to the target hash

value from another block in a case that the target information content does not need to be completely blocked;

[0092] step A9: decoding the target information content, where the target information content may be data serialized in the form of a bit group, and after the target information content is decoded, structural data readable by naked eyes may be obtained, that is, plaintext target information content is obtained;

[0093] step A10: matching the plaintext target information content by using the original index information set, to obtain corresponding target index information, blocking the target index information in the target information content, and then feeding back the target information content with the target index information blocked to the client for display of the client; and

[0094] step A11: directly prompting, in a case that the target information content needs to be completely blocked, the user that the current target information content involves sensitive content and therefore has been blocked. Thus, the embodiment of this application provides a method for detecting a to-be-detected information index by using a variant index information set to obtain a detection result. First, the target hash value is determined according to the to-be-detected information index, and the target hash value is then matched by using the variant index information set. It is determined, in a case that the target hash value successfully matches the variant index information in the variant index information set, the to-be-detected information index is sensitive transaction information, and it is determined, in a case that the target hash value fails to match the variant index information in the variant index information set, that the to-be-detected information index is secure transaction information. In the foregoing manner, when a user requests to browse a designated transaction, a to-be-queried hash value submitted by the user is matched against the variant index information set. Corresponding blocking is performed in a case that the hash value hits the variant index information set, and the transaction information that the user wants to browse is displayed in plaintext form in a case that the hash value does not hit the variant index information set, thereby improving the publication security of the transaction information.

[0095] Optionally, based on the embodiment corresponding to FIG. 3, in a blockchain-based information processing method according to an optional embodiment of s application, the detecting the to-be-detected information index by using the variant index information set, to obtain a detection result, includes:

determining a target intra-block index and a target block height according to the to-be-detected information index;

matching the target intra-block index and the target block height by using the variant index information set;

determining, in a case that the target intra-block index and the target block height successfully match the variant index information in the variant index information set, that the to-be-detected information index is sensitive transaction information; and

determining, in a case that the target intra-block index and the target block height fail to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

[0096] In this embodiment, another manner of detecting the to-be-detected information index is described. For ease of description, the description is made with reference to FIG. 6. FIG. 6 is a schematic flowchart of applying a variant index information set according to an embodiment of this application, which specifically includes:

[0097] step B1: first, obtaining request information initiated by a user, determining a corresponding to-be-detected information index according to the request information, and obtaining a corresponding target block height and a corresponding target intra-block index according to the transaction information;

[0098] step B2: obtaining an updated variant index information set, where because the quantity of blocks is subject to change, the variant index information set is usually updated in real time;

[0099] step B3: matching the target block height and the target intra-block index by using the variant index information set, that is, determining whether the target block height and the target intra-block index hit both a block height and an intra-block index in the variant index information set, where the process proceeds to step B4 in a case that the matching fails, or the process proceeds to step B7 in a case that the matching succeeds;

[0100] step B4: determining, in a case that the target block height and the target intra-block index fail to match variant index information in the variant index information set, that the to-be-detected information index is secure transaction information, where in this case, target information content corresponding to the target block height and the target intra-block index may be obtained from another block;

[0101] step B5: decoding the target information content, where the target information content may be data serialized in the form of a bit group, and after the target information content is decoded, structural data readable by naked eyes may be obtained, that is, plaintext target

information content is obtained;

[0102] step B6: feeding back the plaintext target information content to a client, for display of the client;

5 **[0103]** step B7: determining, in a case that the target block height and the target intra-block index successfully match variant index information in the variant index information set, that the to-be-detected information index is sensitive information, where in this case, it needs to be determined, according to a service requirement, whether the display of target information content needs to be completely blocked, where step B11 is performed in a case that the target information content needs to be completely blocked, or step B8 is performed in a case that the target information
10 content does not need to be completely blocked;

[0104] step B8: obtaining the target information content corresponding to the target block height and the target intra-block index from another block in a case that the target information content does not need to be completely blocked;

15 **[0105]** step B9: decoding the target information content, where the target information content may be data serialized in the form of a bit group, and after the target information content is decoded, structural data readable by naked eyes may be obtained, that is, plaintext target information content is obtained;

20 **[0106]** step B10: matching the plaintext target information content by using the original index information set, to obtain corresponding target index information, blocking the target index information in the target information content, and then feeding back the target information content with the target index information blocked to the client for display of the client; and

[0107] step B11: directly prompting, in a case that the target information content needs to be completely blocked, the user that the current target information content involves sensitive content and therefore has been blocked.

25 **[0108]** Thus, the embodiment of this application provides a method for detecting a to-be-detected information index by using a variant index information set to obtain a detection result. First, the target intra-block index and the target block height are determined according to the to-be-detected information index, and the target intra-block index and the target block height are then matched by using the variant index information set. It is determined, in a case that the target
30 intra-block index and the target block height successfully match the variant index information in the variant index information set, that information corresponding to the to-be-detected information index is sensitive information, and it is determined, in a case that the target intra-block index and

the target block height fail to match the variant index information in the variant index information set, that the information corresponding to the to-be-detected information index is secure information. In the foregoing manner, when a user requests to browse a designated transaction, a to-be-queried intra-block index and a to-be-queried block height that are submitted by the user are matched
5 against the variant index information set. Corresponding blocking is performed in a case that the intra-block index and the block height hit the variant index information set, and the information that the user wants to browse is displayed in plaintext form in a case that the intra-block index and the block height fail to hit the variant index information set, thereby improving the security of information publication.

10 **[0109]** Optionally, based on any of the third embodiment to the fifth embodiment corresponding to FIG. 3, in a blockchain-based information processing method according to an optional embodiment of this application, the processing the request information according to the detection result includes:

obtaining target information content according to the to-be-detected information
15 index in a case that information content corresponding to the to-be-detected information index is secure information; and

transmitting the target information content to a client, to enable the client to display the target information content.

[0110] In this embodiment, based on step A4, step A5, and step A6 in FIG. 5, and step B4,
20 step B5, and step B6 in FIG. 6, when it is determined that the information content corresponding to the to-be-detected information index is the secure information, the target information content corresponding to the to-be-detected information index is obtained according to the request information, that is, the target information content is obtained from another block, the target information content is directly transmitted to the client after decoding, and the target information
25 content is displayed by the client in plaintext form.

[0111] Thus, in the embodiment of this application, a method for processing target information content corresponding to a to-be-detected information index according to a detection result is provided. In a case that the to-be-detected information index is secure transaction information, the target information content is obtained according to the to-be-detected information
30 index, and the target information content is transmitted to the client, to enable the client to display the target information content. In the foregoing manner, for information corresponding to a secure information index, complete information content may be displayed on the client in plaintext form, to provide a user with more complete information while ensuring security, thereby improving the

reliability and feasibility of the solution.

[0112] Optionally, based on any of the embodiments corresponding to FIG. 3, in a blockchain-based information processing method according to an optional embodiment of this application, the processing the request information according to the detection result may include:

5 determining a target sensitivity level and a target service type according to the to-be-detected information index in a case that the information content corresponding to the to-be-detected information index is sensitive information;

 determining, according to the target sensitivity level and the target service type, whether to display the target information content corresponding to the to-be-detected information
10 index;

 transmitting prompt information to the client in a case of determining not to display the target information content, to enable the client to display the prompt information, the prompt information being used for prompting a user that the target information content is the sensitive information; and

15 processing the target information content in a case of determining to display the target information content, to obtain processed target information content.

[0113] In this embodiment, a manner of processing target information content corresponding to a to-be-detected information index according to a detection result is described. A target sensitivity level and a target service type are determined according to the to-be-detected
20 information index in a case that information content corresponding to the to-be-detected information index is sensitive information, and different service requirements usually correspond to different sensitivity levels and service types. Therefore, it is determined, according to the target sensitivity level and the target service type, whether to display the target information content corresponding to the request information. Prompt information is transmitted to the client, for
25 example, "The current transaction information involves sensitive content and is not displayed" in a case that the target information content is not displayed, thereby prompting the user that the target information content is the sensitive transaction information. The target information content is processed in a case that the target information content needs to be displayed, to obtain the processed target information content. That is, target index information in the target information content is
30 blocked, to obtain processed transaction information.

[0114] Specifically, different services may have different requirements on sensitivity levels and service types. Reference is made to Table 6, which is an example of correspondences between

different service requirements, sensitivity levels and service types.

Table 6

Service requirement	Sensitivity level	Service type	Display status
A	Common sensitivity	Electronic contract service	Transaction information is partially displayed
B	High sensitivity	Electronic contract service	Transaction information is not displayed
C	High sensitivity	Bill service	Transaction information is not displayed
D	High sensitivity	Bitcoin service	Transaction information is not displayed
E	Intermediate sensitivity	Electronic contract service	Transaction information is partially displayed

[0115] It may be known from Table 6 that, for the service A, the target sensitivity level is common sensitivity, and the target service type is electronic contract service. In this case, only target index information in the target information content needs to be blocked. For the service B, the target sensitivity level is high sensitivity, and the target service type is electronic contract service. In this case, the target information content needs to be completely blocked.

[0116] Thus, in the embodiment of this application, a method for processing target information content according to a detection result is provided. In a case that the information content corresponding to the to-be-detected information index is the sensitive information, the target sensitivity level and the target service type are determined according to the to-be-detected information index, and it is then determined, according to the target sensitivity level and the target service type, whether to display the target information content corresponding to the to-be-detected information index. The prompt information is transmitted to the client in a case that the target information content is not displayed, to enable the client to display the prompt information, and the target information content is processed in a case that the target information content is displayed, to obtain the processed target information content. In the foregoing manner, it may further be selected, according to a specific service requirement, whether to completely block the sensitive information, thereby improving the flexibility of information processing.

[0117] Optionally, in a blockchain-based information processing method according to an optional embodiment of this application, the processing the target information content, to obtain

processed target information content, may include:

obtaining the target information content;

matching the target information content by using the original index information set, and determining target index information in the target information content; and

5 blocking the target index information in the target information content, to obtain the processed target information content.

[0118] In this embodiment, a manner of processing target information content is described. First, target information content corresponding to a designated hash value is obtained from another block according to the request information. Different from the to-be-detected information index, the
10 target information content is a user-definable field, while the to-be-detected information index is information generated by a system.

[0119] After the target information content is obtained, where it is assumed that the target information content is "A asks B for information about ID card number ", the target information content is matched by using an original index information set. It is determined that target index
15 information in the target information content is "ID card number". Therefore, the target index information is blocked, to obtain processed transaction information, for example, "A asks B for information about *****". The information processing apparatus transmits the processed transaction information to the client, and in this case, the client displays "A asks B for information about *****".

20 **[0120]** Thus, in the embodiment of this application, a method for processing target information content is provided. That is, the target information content is obtained, the target information content is then matched by using the original index information set, the target index information in the target information content is determined, the target index information in the target information content is then blocked to obtain the processed transaction information, and
25 finally, the processed transaction information is transmitted to the client, to enable the client to display the processed transaction information. In the foregoing manner, only some of index information is blocked, thereby improving the security of the information. Meanwhile, the non-index-information part is displayed to facilitate a user to obtain some information, thereby improving the feasibility of the solution.

30 **[0121]** The following describes a blockchain-based information processing method according to this application with reference to the foregoing description. The blockchain-based information processing method may be performed by a blockchain-based data processing apparatus,

and the blockchain-based data processing apparatus is disposed in a network node device. Referring to FIG. 7, the blockchain-based information processing method in an embodiment of this application includes the following steps 201 to 205.

5 **[0122]** Step 201 includes receiving request information, the request information carrying a to-be-detected information index.

10 **[0123]** In this embodiment, when a user requests to display information related to a transaction, the request information may be transmitted through a client, and the information processing apparatus receives the request information. The request information carries the to-be-detected information index, and the to-be-detected information index belongs to an original request.

[0124] Step 202 includes detecting, by using a variant index information set, the to-be-detected information index carried by the request information, to obtain a detection result, the variant index information set including at least one piece of variant index information, the variant index information including an information index in information.

15 **[0125]** In this embodiment, the information processing apparatus detects the to-be-detected information index and the variant index information in the variant index information set, to obtain the detection result. It may be understood that for a manner of detecting the to-be-detected information index in a transaction request, reference may be made to the embodiment corresponding to FIG. 3, which is not described redundantly herein. The variant index information set includes at least one piece of variant index information, and the variant index information is the form of the index. Reference can be made to Table 3, Table 4, and Table 5 for further details, and a generation manner of the variant index information set is shown in the embodiment corresponding to FIG. 3, which are not described redundantly herein.

[0126] In an example, the foregoing step 202 may include the following sub-steps:

25 **[0127]** 1: determining a target hash value according to the to-be-detected information index;

[0128] 2: matching the target hash value by using the variant index information set;

[0129] 3: determining, in a case that the target hash value successfully matches the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive information; and

30 **[0130]** 4: determining, in a case that the target hash value fails to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

[0131] In another embodiment, the foregoing step 202 may include the following sub-steps:

[0132] 1: determining a target intra-block index and a target block height according to the to-be-detected information index;

[0133] 2: matching the target intra-block index and the target block height by using the
5 variant index information set;

[0134] 3: determining, in a case that the target intra-block index and the target block height successfully match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is sensitive transaction information; and

10 **[0135]** 4: determining, in a case that the target intra-block index and the target block height fail to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

[0136] Step 203 includes obtaining information content corresponding to the to-be-detected information index.

15 **[0137]** In this embodiment, the information processing apparatus obtains information content corresponding to the to-be-detected information index, where specifically, the corresponding information content may be obtained from another block.

[0138] Step 204 includes processing the information content corresponding to the to-be-detected information index according to the detection result, to obtain processed information.

20 **[0139]** In this embodiment, the information processing apparatus processes the information content according to the detection result. The information content is directly displayed in plaintext form in a case that the to-be-detected information index indicates that the information content is secure. In a case that the to-be-detected information index indicates that the information content is not secure, the information content may be completely blocked according to a service requirement
25 to obtain the processed transaction information, or the information content is partially blocked to obtain the processed transaction information.

[0140] Optionally, the foregoing step 204 includes the following several sub-steps:

[0141] 1: determining a target sensitivity level and a target service type according to the to-be-detected information index in a case that the information content corresponding to the
30 to-be-detected information index is sensitive information;

[0142] 2: determining, according to the target sensitivity level and the target service type,

whether to display target information content corresponding to the to-be-detected information index;
and

[0143] 3: processing the target information content in a case of determining to display the target information content, to obtain the processed information.

5 [0144] Step 205 includes transmitting the processed transaction information to the client, to enable the client to display the processed transaction information.

[0145] In this embodiment, the information processing apparatus may be disposed in the client or may be disposed outside the client. The information processing apparatus transmits the processed transaction information to the client, to enable the client to display the processed
10 transaction information. The client may be specifically a blockchain browser. For ease of description, reference is made to FIG. 8, which is a schematic flowchart of displaying processed transaction information by a client according to an embodiment of this application, where the information processing apparatus in FIG. 8 is disposed in the client. As shown in FIG. 8, the flowchart specifically includes steps C1 to C6.

15 [0146] In step C1, a user triggers, by using a client, a request, that is, a request for viewing information related to a transaction.

[0147] In step C2, the information processing apparatus searches for another related block by using a local block;

[0148] In step C3, the information processing apparatus decodes block information on the
20 related block according to the request initiated by the user, to obtain transaction information.

[0149] In step C4, the information processing apparatus matches the transaction information against variant index information in a variant index information set.

[0150] In step C5, sensitive content, for example, a sensitive phrase or a sensitive word, in the information is blocked in a case that the sensitive content exists in the information.

25 [0151] In step C6, the information processing apparatus displays, to the user, information obtained after the blocking.

[0152] Optionally, the foregoing method may further include the following steps:

[0153] 1: obtaining an original index information set, the original index information set including at least one piece of original index information, each piece of original index information
30 including plaintext sensitive content;

[0154] 2: obtaining information in to-be-matched blocks, the information including

information content and an information index, the information content having a correspondence with the information index;

[0155] 3: matching the information content in the information by using the original index information set, to obtain a matching result; and

5 **[0156]** 4: generating the variant index information set according to the matching result in a case that the matching result indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index information including the information index corresponding to the information content in the information.

[0157] Optionally, the step includes the following sub-steps:

10 **[0158]** 4.1: obtaining a sensitivity level of the original index information in a case that the matching result is that the information successfully matches the original index information in the original index information set;

[0159] 4.2: obtaining a hash value, an intra-block index, and a block height in the information index, the intra-block index representing a position of the information in the
15 to-be-matched block; and

[0160] 4.3: generating the variant index information set according to the sensitivity level of the original index information, the hash value, the intra-block index, and the block height.

[0161] For an obtaining process of the detection result, an obtaining procedure of the processed information, and a generation manner of the variant index information set, refer may be
20 made to the foregoing embodiments, which are not described redundantly herein.

[0162] In the embodiment of this application, a blockchain-based information processing method is provided. First, a transaction request transmitted by a client is received, and a to-be-detected information index carried by the transaction request is then detected by using a variant index information set, to obtain a detection result, target information content corresponding
25 to the to-be-detected information index is obtained, finally, the target information content is processed according to the detection result, to obtain processed transaction information, and the processed transaction information is transmitted to the client, to enable the client to display the processed transaction information. In the foregoing manner, the transaction information is detected by using the variant index information set, so that the risk brought to a blockchain application by
30 security supervision on blockchain content can be effectively resolved, so that index information can be transmitted to providers of blockchain services while avoiding potential security hazards brought by direct transmission of the original index information set. In addition, the transaction may

further be processed, to obtain the processed transaction information, and the transmission of the processed transaction information can further improve the security of the solution.

[0163] Optionally, an embodiment of this application provides a blockchain-based information processing method. The method includes the following steps:

5 **[0164]** first step: receiving request information, the request information carrying a to-be-detected information index;

[0165] second step: determining a target intra-block index and a target block height according to the to-be-detected information index;

10 **[0166]** third step: matching the target intra-block index and the target block height by using a variant index information set, the variant index information set including at least one piece of variant index information, the variant index information including an information index corresponding to information content in information;

15 **[0167]** fourth step: determining, in a case that the target intra-block index and the target block height successfully match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is sensitive transaction information;

20 **[0168]** fifth step: determining, in a case that the target intra-block index and the target block height fail to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information; and

[0169] sixth step: processing the request information according to the detection result.

[0170] For descriptions of the foregoing steps, reference may be made to the embodiments above, which are not described redundantly herein.

25 **[0171]** A blockchain-based information processing apparatus of this application is described below in detail. Reference is made to FIG. 9, which is a schematic diagram of a blockchain-based information processing apparatus according to an embodiment of this application. The information processing apparatus 30 includes:

30 an obtaining module 301, configured to obtain an original index information set, the original index information set including at least one piece of original index information, each piece of original index information including plaintext sensitive content,

the obtaining module 301 being further configured to obtain information in

to-be-matched blocks, the information including information content and an information index, the information content having a correspondence with the information index;

a matching module 302, configured to match the information content in the information by using the original index information set obtained by the obtaining module 301, to obtain a matching result; and

a generation module 303, configured to generate a variant index information set according to the matching result in a case that the matching result obtained by the matching module 302 indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index information including the information index corresponding to the information content in the information.

[0172] In this embodiment, the obtaining module 301 obtains an original index information set, the original index information set including at least one piece of original index information, each piece of original index information including plaintext sensitive content; the obtaining module 301 obtains information in to-be-matched blocks, the information including information content and an information index, the information content having a correspondence with the information index; the matching module 302 matches the information content in the information by using the original index information set obtained by the obtaining module 301, to obtain a matching result; and the generation module 303 generates a variant index information set according to the matching result in a case that the matching result obtained by the matching module 302 indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index information including the information index corresponding to the information content in the information.

[0173] In the embodiments of this application, a blockchain-based information processing apparatus is provided. First, an original index information set is obtained, the original index information set including at least one piece of original index information, each piece of original index information including plaintext sensitive content; information in to-be-matched blocks is then obtained, the information including information content and an information index, the information content having a correspondence with the information index; and the information content in the information is matched by using the original index information set, to obtain a matching result, and a variant index information set is generated according to the matching result in a case that the matching result indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index information including the information index corresponding to the information content in the information. Through the foregoing manner, a

record of index information is no longer maintained in plaintext form, but an information index of the index information involved during a blockchain transaction is recorded, thereby forming variant index information. The variant index information does not directly display specific content of the index information, but is maintained in the form of the information index, so that potential security hazards are less likely to arise, and the security of information maintenance is improved.

[0174] Optionally, based on the embodiment corresponding to FIG. 9, in the information processing apparatus 30 according to another embodiment of this application,

the matching module 302 is specifically configured to: match first information content by using the original index information set, the first information content belonging to the information; and

match information content in a second block in a case that the first information content is the last piece of information in a first block, the first block being a block of the to-be-matched blocks, the second block being another block of the to-be-matched blocks, the second block being a next block adjacent to the first block; or

obtain second information content in the first block in a case that the first information content is not the last piece of information in the first block, and match the second information content by using the original index information set, the second information content being a next piece of information content adjacent to the first information content.

[0175] Thus, in the embodiment of this application, a method for matching transaction information by using an original index information set is provided. That is, the first information content is matched by using the original index information set. The information content in the second block is matched in a case that the first information content is the last piece of transaction information in the first block, and in a case that the first information content is not the last piece of transaction information in the first block, the second information content in the first block is obtained and matched by using the original index information set. Through the foregoing method, during actual matching, each piece of information content in each block is matched, to achieve a full scan of the block, thereby facilitating the generation of a more complete variant index information set.

[0176] Optionally, based on the embodiment corresponding to FIG. 9, in the information processing apparatus 30 according to another embodiment of this application,

the generation module 303 is specifically configured to: obtain a sensitivity level of the original index information in a case that the matching result is that the information successfully

matches the original index information in the original index information set;

obtain a hash value, an intra-block index, and a block height in the information index, the intra-block index representing a position of the information in the to-be-matched block; and

5 generate the variant index information set according to the sensitivity level of the original index information, the hash value, the intra-block index, and the block height.

[0177] Thus, in the embodiment of this application, a manner of generating a variant index information set is provided. The sensitivity level of the original index information is obtained in a case that the matching result is that the information content successfully matches the original index information in the original index information set, and the hash value, the intra-block index, and the block height in the information index may then be obtained. The intra-block index represents a position of the information content in the to-be-matched block. Finally, the variant index information set may be generated according to the sensitivity level of the original index information, the hash value, the intra-block index, and the block height. Alternatively, the variant index information set may be generated according to the sensitivity level of the original index information and the hash value. Alternatively, the variant index information set may be generated according to the sensitivity level of the original index information, the intra-block index, and the block height. In the foregoing manner, the generated variant index information set may include different information. Three types of usable variant index information sets are listed herein, and information matching may be performed according to an actual requirement, thereby improving the flexibility and applicability of the solution.

[0178] Optionally, based on the embodiment corresponding to FIG. 9, referring to FIG. 10, in another embodiment of this application, the information processing apparatus 30 further includes a processing module 304, where

25 the processing module 304 is configured to: receive request information after the generation module 303 generates the variant index information set according to the matching result, the request information carrying a to-be-detected information index;

detect the to-be-detected information index by using the variant index information set, to obtain a detection result; and

process the request information according to the detection result.

30 [0179] Thus, in the embodiment of this application, an application method of a variant index information set is provided. After the variant index information set is generated, the request information transmitted by a client may further be received, the to-be-detected information index is

then detected by using the variant index information set to obtain the detection result, and finally, the request information is processed according to the detection result. In the foregoing manner, the information index is detected by using the variant index information set, so that the risk brought to a blockchain application by security supervision on blockchain content can be effectively resolved, so that the information index is transmitted to providers of blockchain services while avoiding potential security hazards brought by direct transmission of original index information.

[0180] Further, an embodiment of this application provides a method for detecting a to-be-detected information index by using a variant index information set to obtain a detection result. First, a target hash value is determined according to the to-be-detected information index, and the target hash value is then matched by using the variant index information set. It is determined, in a case that the target hash value successfully matches the variant index information in the variant index information set, the to-be-detected information index is sensitive transaction information, and it is determined, in a case that the target hash value fails to match the variant index information in the variant index information set, that the to-be-detected information index is secure transaction information. In the foregoing manner, when a user requests to browse a designated transaction, a to-be-queried hash value submitted by the user is matched against the variant index information set. Corresponding blocking is performed in a case that the hash value hits the variant index information set, and the transaction information that the user wants to browse is displayed in plaintext form in a case that the hash value does not hit the variant index information set, thereby improving the publication security of the transaction information.

[0181] Optionally, based on the embodiment corresponding to FIG. 10, in the information processing apparatus 30 according to another embodiment of this application,

the processing module 304 is specifically configured to: determine a target hash value according to the to-be-detected information index;

match the target hash value by using the variant index information set;

determine, in a case that the target hash value successfully matches the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive information; and

determine, in a case that the target hash value fails to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

[0182] Further, an embodiment of this application provides a method for detecting a

to-be-detected information index by using a variant index information set to obtain a detection result. First, a target intra-block index and a target block height are determined according to the to-be-detected information index, and the target intra-block index and the target block height are then matched by using the variant index information set. It is determined, in a case that the target
5 intra-block index and the target block height successfully match the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive information, and it is determined, in a case that the target intra-block index and the target block height fail to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index
10 is secure information. In the foregoing manner, when a user requests to browse a designated transaction, a to-be-queried intra-block index and a to-be-queried block height that are submitted by the user are matched against the variant index information set. Corresponding blocking is performed in a case that the intra-block index and the block height hit the variant index information set, and the information that the user wants to browse is displayed in plaintext form in a case that
15 the intra-block index and the block height fail to hit the variant index information set, thereby improving the publication security of information.

[0183] Optionally, based on the embodiment corresponding to FIG. 10, in the information processing apparatus 30 according to another embodiment of this application,

the processing module 304 is specifically configured to: determine a target
20 intra-block index and a target block height according to the to-be-detected information index;

match the target intra-block index and the target block height by using the variant index information set;

determine, in a case that the target intra-block index and the target block height successfully match the variant index information in the variant index information set, that the
25 to-be-detected information index is sensitive transaction information; and

determine, in a case that the target intra-block index and the target block height fail to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

[0184] Further, the embodiment of this application provides a method for detecting a
30 to-be-detected information index by using a variant index information set to obtain a detection result. First, the target intra-block index and the target block height are determined according to the to-be-detected information index, and the target intra-block index and the target block height are

then matched by using the variant index information set. It is determined, in a case that the target intra-block index and the target block height successfully match the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive information, and it is determined, in a case that the target intra-block index and the target block height fail to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information. In the foregoing manner, when a user requests to browse a designated transaction, a to-be-queried intra-block index and a to-be-queried block height that are submitted by the user are matched against the variant index information set. Corresponding blocking is performed in a case that the intra-block index and the block height hit the variant index information set, and the information that the user wants to browse is displayed in plaintext form in a case that the intra-block index and the block height fail to hit the variant index information set, thereby improving the security of information publication.

[0185] Optionally, based on the embodiment corresponding to FIG. 10, in the information processing apparatus 30 according to another embodiment of this application,

the processing module 304 is specifically configured to: obtain target information content according to the to-be-detected information index in a case that information content corresponding to the to-be-detected information index is secure information; and

transmit the target information content to a client, to enable the client to display the target information content.

[0186] Thus, in the embodiment of this application, a method for processing target information content corresponding to a to-be-detected information index according to a detection result is provided. In a case that the to-be-detected information index is secure transaction information, the target information content is obtained according to the to-be-detected information index, and the target information content is transmitted to the client, to enable the client to display the target information content. In the foregoing manner, for information corresponding to a secure information index, complete information content may be displayed on the client in plaintext form, to provide a user with more complete information while ensuring security, thereby improving the reliability and feasibility of the solution.

[0187] Optionally, based on the embodiment corresponding to FIG. 10, in the information processing apparatus 30 according to another embodiment of this application,

the processing module 304 is specifically configured to: determine a target

sensitivity level and a target service type according to the to-be-detected information index in a case that the information content corresponding to the to-be-detected information index is sensitive information;

5 determine, according to the target sensitivity level and the target service type, whether to display the target information content corresponding to the to-be-detected information index;

10 transmit prompt information to the client in a case of determining not to display the target information content, to enable the client to display the prompt information, the prompt information being used for prompting a user that the target information content is the sensitive information; and

 process the target information content in a case of determining to display the target information content, to obtain processed target information content, and transmit the processed target information content to the client, to enable the client to display the processed target information content.

15 **[0188]** Thus, in the embodiment of this application, a method for processing target information content according to a detection result is provided. In a case that the information content corresponding to the to-be-detected information index is the sensitive information, the target sensitivity level and the target service type are determined according to the to-be-detected information index, and it is then determined, according to the target sensitivity level and the target service type, whether to display the target information content corresponding to the to-be-detected information index. The prompt information is transmitted to the client in a case that the target information content is not displayed, to enable the client to display the prompt information, and the target information content is processed in a case that the target information content is displayed, to obtain the processed target information content. In the foregoing manner, it may further be selected, according to a specific service requirement, whether to completely block the sensitive information, thereby improving the flexibility of information processing.

[0189] Optionally, based on the embodiment corresponding to FIG. 10, in the information processing apparatus 30 according to another embodiment of this application,

 the processing module 304 is specifically configured to: obtain the target information content;
30 match the target information content by using the original index information set, and determine target index information in the target information content; and
 block the target index information in the target information content, to obtain the

processed target information content.

[0190] Thus, in the embodiment of this application, a method for processing target information content is provided. That is, the target information content is obtained, the target information content is then matched by using the original index information set, the target index information in the target information content is determined, the target index information in the target information content is then blocked, to obtain the processed transaction information, and finally, the processed transaction information is transmitted to the client, to enable the client to display the processed transaction information. In the foregoing manner, only some of index information is blocked, thereby improving the security of the information. Meanwhile, the non-index-information part is displayed to help a user obtain some information, thereby improving the feasibility of the solution.

[0191] A blockchain-based information processing apparatus in the embodiments of this application is described below in detail. Reference is made to FIG. 11, which is a schematic diagram of a blockchain-based information processing apparatus according to an embodiment of this application. The information processing apparatus 40 includes:

a receiving module 401, configured to receive request information, the request information carrying a to-be-detected information index;

a detection module 402, configured to detect, by using a variant index information set, the to-be-detected information index carried by the request information received by the receiving module 401, to obtain a detection result, the variant index information set including at least one piece of variant index information, the variant index information including an information index in information;

an obtaining module 403, configured to obtain information content corresponding to the to-be-detected information index;

a processing module 404, configured to process, according to the detection result detected by the detection module 402, the information content corresponding to the to-be-detected information index obtained by the obtaining module 403, to obtain processed transaction information; and

a transmission module 405, configured to transmit the processed transaction information obtained by the processing module 404 to the client, to enable the client to display the processed transaction information.

[0192] Optionally, the detection module 402 is configured to:

determine a target hash value according to the to-be-detected information index;

match the target hash value by using the variant index information set;

determine, in a case that the target hash value successfully matches the variant index information in the variant index information set, that information content corresponding to the

5 to-be-detected information index is sensitive information; and

determine, in a case that the target hash value fails to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

[0193] Optionally, the detection module 402 is configured to:

10 determine a target intra-block index and a target block height according to the to-be-detected information index;

match the target intra-block index and the target block height by using the variant index information set;

15 determine, in a case that the target intra-block index and the target block height successfully match the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive transaction information; and

20 determine, in a case that the target intra-block index and the target block height fail to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

[0194] Optionally, the processing module 404 is configured to:

determine a target sensitivity level and a target service type according to the to-be-detected information index in a case that the information content corresponding to the to-be-detected information index is sensitive information;

25 determine, according to the target sensitivity level and the target service type, whether to display target information content corresponding to the to-be-detected information index; and

process the target information content in a case of determining to display the target information content, to obtain the processed information.

30 **[0195]** Optionally, the information processing apparatus 40 further includes: a matching

module and a generation module (not shown in the drawings).

[0196] The obtaining module 403 is further configured to obtain an original index information set, the original index information set including at least one piece of original index information, each piece of original index information including plaintext sensitive content.

5 **[0197]** The obtaining module 403 is further configured to obtain information in to-be-matched blocks, the information including information content and an information index, the information content having a correspondence with the information index.

[0198] The matching module is configured to match the information content in the information by using the original index information set, to obtain a matching result.

10 **[0199]** The generation module is configured to generate the variant index information set according to the matching result in a case that the matching result indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index information including the information index corresponding to the information content in the information.

15 **[0200]** Optionally, the generation module is configured to:

obtain a sensitivity level of the original index information in a case that the matching result is that the information successfully matches the original index information in the original index information set;

20 obtain a hash value, an intra-block index, and a block height in the information index, the intra-block index representing a position of the information in the to-be-matched block; and

generate the variant index information set according to the sensitivity level of the original index information, the hash value, the intra-block index, and the block height.

[0201] In this embodiment, the receiving module 401 receives request information, the request information carrying a to-be-detected information index; the detection module 402 detects, 25 by using a variant index information set, the to-be-detected information index carried by the request information received by the receiving module 401, to obtain a detection result, the variant index information set including at least one piece of variant index information, the variant index information including an information index in information; the obtaining module 403 obtains information content corresponding to the to-be-detected information index; the processing module 30 404 processes, according to the detection result detected by the detection module 402, the information content corresponding to the to-be-detected information index obtained by the obtaining module 403, to obtain processed transaction information; and the transmission module

405 transmits the processed transaction information obtained by the processing module 404 to the client, to enable the client to display the processed transaction information.

[0202] In the embodiment of this application, a blockchain-based information processing method is provided. First, a transaction request transmitted by a client is received, and a
5 to-be-detected information index carried by the transaction request is then detected by using a variant index information set, to obtain a detection result, target information content corresponding to the to-be-detected information index is obtained, finally, the target information content is processed according to the detection result, to obtain processed transaction information, and the processed transaction information is transmitted to the client, to enable the client to display the
10 processed transaction information. In the foregoing manner, the transaction information is detected by using the variant index information set, so that the risk brought to a blockchain application by security supervision on blockchain content can be effectively resolved, and index information can be transmitted to providers of blockchain services while avoiding potential security hazards brought by direct transmission of the original index information set. In addition, the transaction may further
15 be processed, to obtain the processed transaction information, and the transmission of the processed transaction information can further improve security of the solution.

[0203] FIG. 12 is a schematic structural diagram of a network node device according to an embodiment of this application. The network node device 500 may vary greatly due to different configurations or performance, and may include one or more central processing units (CPU) 522
20 (for example, one or more processors), a memory 532, and one or more storage media 530 (for example, one or more mass storage devices) that store programs 542 or data 544. The memory 532 and the storage medium 530 may be a temporary storage or a persistent storage. The program stored in the storage medium 530 may include one or more modules (not shown in the drawings), and each module may include a series of instructions and operations for the network node device.
25 Furthermore, the CPU 522 may be configured to communicate with the storage mediums 530, and perform, on the network node device 500, the series of instruction operations in the storage mediums 530.

[0204] The network node device 500 may further include one or more power supplies 526, one or more wired or wireless network interfaces 550, one or more input/output interfaces 558,
30 and/or one or more operating systems 541, for example, Windows Server™, Mac OS X™, Unix™, Linux™ or FreeBSD™.

[0205] Steps performed by the network node device in the foregoing embodiments may be based on the structure of the network node device shown in FIG. 12.

[0206] In an embodiment of this application, the CPU 522 is configured to perform the following steps:

obtaining an original index information set, the original index information set including at least one piece of original index information, each piece of original index information including plaintext sensitive content;

obtaining information in to-be-matched blocks, the information including information content and an information index, the information content having a correspondence with the information index;

matching the information content in the information by using the original index information set, to obtain a matching result; and

generating a variant index information set according to the matching result in a case that the matching result indicates that the matching succeeds, the variant index information set including at least one piece of variant index information, the variant index information including the information index corresponding to the information content in the information.

[0207] In an embodiment of this application, the CPU 522 is configured to perform the following steps:

receiving request information, the request information carrying a to-be-detected information index;

detecting, by using a variant index information set, the to-be-detected information index carried by the request information, to obtain a detection result, the variant index information set including at least one piece of variant index information, the variant index information including an information index in information;

obtaining information content corresponding to the to-be-detected information index;

processing the information content corresponding to the to-be-detected information index according to the detection result, to obtain processed transaction information; and

transmitting the processed transaction information to the client, to enable the client to display the processed transaction information.

[0208] A person skilled in the art may clearly understand that, for the purpose of convenient and brief description, for specific work processes of the foregoing described system, apparatus, and unit, reference may be made to corresponding processes in the foregoing method embodiments, which are not described herein again.

[0209] In the embodiments in this application, it is to be understood that the disclosed system, apparatus, and method may be implemented in other manners. For example, the described apparatus embodiment is merely an example. For example, the unit division is merely logical function division and there may be other divisions during actual implementation. For example, a plurality of units or components may be combined or integrated into another system, or some features may be ignored or not performed. In addition, the displayed or discussed mutual couplings or direct couplings or communication connections may be implemented by using some interfaces. The indirect couplings or communication connections between the apparatus or units may be implemented in electronic, mechanical, or other forms.

[0210] The units described as separate parts may or may not be physically separate. Parts displayed as units may or may not be physical units, which may be located in one position, or be distributed on a plurality of network units. Some or all of the units can be selected according to actual requirements to achieve the objectives of the solutions in the embodiments.

[0211] In addition, functional units in the embodiments of this application may be integrated into one processing unit, or each of the units may exist alone physically, or two or more units are integrated into one unit. The integrated unit may be implemented in the form of hardware, or may be implemented in the form of a software function unit.

[0212] When the integrated unit is implemented in the form of a software functional unit and sold or used as an independent product, the integrated unit may be stored in a computer-readable storage medium. Based on such an understanding, the technical solutions of this application essentially, or the part contributing to the related art, or the entire or some of the technical solutions may be implemented in a form of a software product. The computer software product is stored in a storage medium and includes several instructions for instructing a computer device (which may be a PC, a server, a network device, or the like) to perform all or some of the steps of the methods described in the embodiments of this application. The foregoing storage medium includes: any medium that can store program code, such as a USB flash drive, a portable hard disk, a read-only memory (read-only memory, ROM), a random access memory (random access memory, RAM), a magnetic disk, or an optical disc.

[0213] The foregoing embodiments are merely provided for describing the technical solutions of this application, but not intended to limit this application. A person of ordinary skill in the art shall understand that although this application has been described in detail with reference to the foregoing embodiments, modifications can be made to the technical solutions described in the foregoing embodiments, or equivalent replacements can be made to some technical features in the

technical solutions, and that such modifications or replacements do not cause the essence of corresponding technical solutions to depart from the spirit and scope of the technical solutions of the embodiments of this application.

CLAIMS

What is claimed is:

1. A blockchain-based information processing method, performed by a network node device, the method comprising:

obtaining an original index information set, the original index information set comprising at least one piece of original index information, each piece of original index information comprising plaintext sensitive content;

obtaining information in to-be-matched blocks, the information comprising information content and an information index, the information content having a correspondence with the information index;

matching the information content in the information by using the original index information set, to obtain a matching result; and

generating a variant index information set according to the matching result in a case that the matching result indicates that the matching succeeds, the variant index information set comprising at least one piece of variant index information, the variant index information comprising the information index corresponding to the information content in the information.

2. The method according to claim 1, wherein the matching the information content in the information by using the original index information set comprises:

matching first information content by using the original index information set, the first information content belonging to the information; and

matching information content in a second block in a case that the first information content is the last piece of information in a first block, the first block being a block of the to-be-matched blocks, the second block being another block of the to-be-matched blocks, the second block being a next block adjacent to the first block; or

obtaining second information content in the first block in a case that the first information content is not the last piece of information in the first block, and matching the second information content by using the original index information set, the second information content being a next piece of information content adjacent to the first information content.

3. The method according to claim 1, wherein the generating a variant index information set according to the matching result comprises:

obtaining a sensitivity level of the original index information in a case that the matching result is that the information successfully matches the original index information in the original index information set;

obtaining a hash value, an intra-block index, and a block height in the information index, the intra-block index representing a position of the information in the to-be-matched block; and

generating the variant index information set according to the sensitivity level of the original index information, the hash value, the intra-block index, and the block height.

4. The method according to claim 3, wherein after the generating a variant index information set according to the matching result, the method further comprises:

receiving request information, the request information carrying a to-be-detected information index;

detecting the to-be-detected information index by using the variant index information set to obtain a detection result; and

processing the request information according to the detection result.

5. The method according to claim 4, wherein the detecting the to-be-detected information index by using the variant index information set to obtain a detection result comprises:

determining a target hash value according to the to-be-detected information index;

matching the target hash value by using the variant index information set;

determining, in a case that the target hash value successfully matches the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive information; and

determining, in a case that the target hash value fails to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

6. The method according to claim 4, wherein the detecting the to-be-detected information index by using the variant index information set to obtain a detection result comprises:

determining a target intra-block index and a target block height according to the to-be-detected information index;

matching the target intra-block index and the target block height by using the variant index information set;

determining, in a case that the target intra-block index and the target block height successfully match the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive transaction information; and

determining, in a case that the target intra-block index and the target block height fail to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

7. The method according to any one of claims 4 to 6, wherein the processing the request information according to the detection result comprises:

obtaining target information content according to the to-be-detected information index in a case that information content corresponding to the to-be-detected information index is secure information; and

transmitting the target information content to a client, to enable the client to display the target information content.

8. The method according to claim 7, wherein the processing the request information according to the detection result comprises:

determining a target sensitivity level and a target service type according to the to-be-detected information index in a case that the information content corresponding to the to-be-detected information index is sensitive information;

determining, according to the target sensitivity level and the target service type, whether to display the target information content corresponding to the to-be-detected information index;

transmitting prompt information to the client in a case of determining not to display the target information content, to enable the client to display the prompt information, the prompt information being used for prompting a user that the target information content is the sensitive information; and

processing the target information content in a case of determining to display the target information content to obtain processed target information content, and transmitting the processed target information content to the client, to enable the client to display the processed target information content.

9. The method according to claim 8, wherein the processing the target information content to obtain processed target information content comprises:

obtaining the target information content;

matching the target information content by using the original index information set, and

determining target index information in the target information content; and

blocking the target index information in the target information content, to obtain the processed target information content.

10. A blockchain-based information processing method, performed by a network node device, the method comprising:

receiving request information, the request information carrying a to-be-detected information index;

detecting, by using a variant index information set, the to-be-detected information index carried by the request information to obtain a detection result, the variant index information set comprising at least one piece of variant index information, the variant index information comprising an information index in information;

obtaining information content corresponding to the to-be-detected information index;

processing the information content corresponding to the to-be-detected information index according to the detection result to obtain processed information; and

transmitting the processed information, to display the processed information.

11. The method according to claim 10, wherein the detecting, by using a variant index information set, the to-be-detected information index carried by the request information to obtain a detection result comprises:

determining a target hash value according to the to-be-detected information index;

matching the target hash value by using the variant index information set;

determining, in a case that the target hash value successfully matches the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive information; and

determining, in a case that the target hash value fails to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

12. The method according to claim 10, wherein the detecting, by using a variant index information set, the to-be-detected information index carried by the request information to obtain a detection result comprises:

determining a target intra-block index and a target block height according to the to-be-detected

information index;

matching the target intra-block index and the target block height by using the variant index information set;

determining, in a case that the target intra-block index and the target block height successfully match the variant index information in the variant index information set, that information content corresponding to the to-be-detected information index is sensitive transaction information; and

determining, in a case that the target intra-block index and the target block height fail to match the variant index information in the variant index information set, that the information content corresponding to the to-be-detected information index is secure information.

13. The method according to claim 10, wherein the processing the information content corresponding to the to-be-detected information index according to the detection result to obtain processed information comprises:

determining a target sensitivity level and a target service type according to the to-be-detected information index in a case that the information content corresponding to the to-be-detected information index is sensitive information;

determining, according to the target sensitivity level and the target service type, whether to display target information content corresponding to the to-be-detected information index; and

processing the target information content in a case of determining to display the target information content, to obtain the processed information.

14. The method according to any one of claims 10 to 13, wherein the method further comprises:

obtaining an original index information set, the original index information set comprising at least one piece of original index information, each piece of original index information comprising plaintext sensitive content;

obtaining information in to-be-matched blocks, the information comprising information content and an information index, the information content having a correspondence with the information index;

matching the information content in the information by using the original index information set, to obtain a matching result; and

generating the variant index information set according to the matching result in a case that the matching result indicates that the matching succeeds, the variant index information set comprising

at least one piece of variant index information, the variant index information comprising the information index corresponding to the information content in the information.

15. The method according to claim 14, wherein the generating the variant index information set according to the matching result comprises:

obtaining a sensitivity level of the original index information in a case that the matching result is that the information successfully matches the original index information in the original index information set;

obtaining a hash value, an intra-block index, and a block height in the information index, the intra-block index representing a position of the information in the to-be-matched block; and

generating the variant index information set according to the sensitivity level of the original index information, the hash value, the intra-block index, and the block height.

16. A blockchain-based data processing apparatus, comprising:

an obtaining module, configured to obtain an original index information set, the original index information set comprising at least one piece of original index information, each piece of original index information comprising plaintext sensitive content,

the obtaining module being further configured to obtain information in to-be-matched blocks, the information comprising information content and an information index, the information content having a correspondence with the information index;

a matching module, configured to match the information content in the information by using the original index information set obtained by the obtaining module, to obtain a matching result; and

a generation module, configured to generate a variant index information set according to the matching result in a case that the matching result obtained by the matching module indicates that the matching succeeds, the variant index information set comprising at least one piece of variant index information, the variant index information comprising the information index corresponding to the information content in the information.

17. A blockchain-based data processing apparatus, comprising:

a receiving module, configured to receive request information, the request information carrying a to-be-detected information index;

a detection module, configured to detect, by using a variant index information set, the to-be-detected information index carried by the request information, to obtain a detection result, the

variant index information set comprising at least one piece of variant index information, the variant index information comprising an information index in information;

an obtaining module, configured to obtain information content corresponding to the to-be-detected information index;

a processing module, configured to process the information content corresponding to the to-be-detected information index according to the detection result, to obtain processed information; and

a transmission module, configured to transmit the processed information, to display the processed information.

18. A network node device, comprising a memory and a processor,

the memory being configured to store a program;

the processor being configured to perform the method according to any one of claims 1 to 9 by executing the program in the memory.

19. A network node device, comprising a memory and a processor,

the memory being configured to store a program;

the processor being configured to perform the method according to any one of claims 10 to 15 by executing the program in the memory.

20. A computer-readable storage medium, comprising instructions, the instructions, when run on a computer, causing the computer to perform the method according to any one of claims 1 to 9 or the method according to any one of claims 10 to 15.