

Description

Title of Invention: BLOCKCHAIN DATA SEARCH METHOD

Technical Field

- [1] The present invention relates generally to a data search method in a blockchain network.

Background Art

- [2] Recently, the fourth industrial revolution has become an issue through the convergence of information and communication technologies. Automation in the existing industry means that a machine passively operates according to a program input in advance. Meanwhile, automation in the fourth industrial revolution means that a machine actively identifies a situation and operates according thereto. The fourth industrial revolution is led by artificial intelligence, robot technology, and life science. Particularly, the blockchain, which is attracting attention as a core element technology of the fourth industrial revolution, is a technology that manages files that record transaction information in a P2P network, in a distributed manner.
- [3] Since such blockchain technology can store information in a distributed manner, the blockchain technology has attracted attention as a technology for storing general information as well as transaction records.
- [4] However, various operating entities operate their respective blockchain networks, and users must access each blockchain network when they want to search for information. Herein, searching each blockchain network for information is not easy for general users, not experts such as programmers.
- [5] In this regard, Korean Patent Application Publication No. 10-2019-0096231 discloses a blockchain-based information management and providing system, the system including: first and second file storages encrypting and storing customer information encrypting and storing customer information including medical information and product purchase information; a key storage server generating and storing an encryption key for encrypted customer information stored in the first and second file storage and storing pre-stored customer signature information in order to determine whether the customer has approved the sharing and disclosure of encrypted customer information; a metadata server generating a virtual file by matching the customer identification information (ID) corresponding to the encrypted customer information; a search server preparing a list of encrypted customer information and disclosing customer information in each list when a customer approves the sharing and disclosure of customer information, and cataloging the disease distribution by customer's gender and age and products with high sales volume and preventing detailed customer in-

formation from being disclosed when the customer does not approve the sharing and disclosure of customer information, in response to a search expression based on the first and second file storage; and a management server controlling the combination of the encrypted customer information in the first and second file storage, controlling approval of the sharing and disclosure of customer information from customers, and encrypted customer information.

- [6] The patent document merely provides a system for storing and managing information in a specific manner, and does not enable users to conveniently search across multiple blockchain networks.

Disclosure of Invention

Technical Problem

- [7] An embodiment of the present invention has an objective to provide a method by which a user easily can search for data stored in a block without directly accessing the blockchain network.

Solution to Problem

- [8] A blockchain data search method according to an embodiment of the present invention includes receiving a search term for identifying a block from a user terminal, and selecting a blockchain network to be searched from among multiple blockchain networks; accessing the selected blockchain network to enter the search term and thus searching the selected blockchain network for a block corresponding to the search term; receiving data stored in the searched block from the selected blockchain network; and transmitting the received data to the user terminal, wherein the search term may be a hash value or a block number.
- [9] The search term may be entered in a form of a QR code.
- [10] The receiving may include receiving the search term from the user terminal and then providing the user terminal with blockchain network candidates in which a block is capable of being searched for using the search term on the basis of a type of the search term; and selecting any one from among the blockchain network candidates as the blockchain network by the user terminal.
- [11] The transmitting the received data to the user terminal may include, when the data stored in the found block is a URL link, accessing a specific data storage server corresponding to the URL link to transmit data received from the specific data storage server to the user terminal.
- [12] The data received from the specific data storage server may be an image or a video.
- [13] The transmitting the received data to the user terminal may include, when the data stored in the found block indicates a specific service, executing a client of the specific service to transmit the received data to the user terminal.

[14] The specific service may be at least one of a messenger service, a news providing service, a music providing service, and a game.

[15] The method may further include, between the receiving of the search term and the accessing of the selected blockchain network, receiving a private key from the user terminal, to release security of the selected blockchain network using the received private key and a public key.

Advantageous Effects of Invention

[16] According to an embodiment of the present invention, a user can easily search for data stored in a block by simply entering a search term and a blockchain network name without having to directly access the blockchain network.

[17] According to an embodiment of the present invention, when data stored in a block is a URL link, a user can directly receive an image, a video, etc. stored in a data storage server corresponding to an URL link without a procedure of accessing the URL link.

[18] According to an embodiment of the present invention, when data stored in a block corresponds to a specific service, a user can directly receive a result of executing specific service without executing the specific service.

Brief Description of Drawings

[19] FIG. 1 is a diagram showing the configuration of a blockchain search system according to an embodiment of the present invention.

[20] FIG. 2 is a diagram showing an example of a structure of a block generated at a node of FIG. 1.

[21] FIG. 3 is a diagram showing an example of a structure of a block generated at a node of FIG. 1.

[22] FIG. 4 is a flowchart showing a blockchain search method according to an embodiment of the present invention.

[23] FIGS. 5a, 5b and 5c are diagrams showing screens of user terminals in which a blockchain search method is implemented according to an embodiment of the present invention.

[24] FIG. 6 is a diagram showing a screen of a user terminal in which a blockchain search method is implemented according to an embodiment of the present invention, which is a screen showing other search results.

[25] FIG. 7 is a diagram showing a screen of a user terminal in which a blockchain search method is implemented according to an embodiment of the present invention, which is a screen showing other search results.

[26] FIG. 8 is a diagram showing a screen of a user terminal in which a blockchain search method is implemented according to an embodiment of the present invention, which is a screen showing other search results.

Mode for the Invention

- [27] Based on the principle that the inventor can appropriately define the concept of terms in order to explain his or her invention in the best way, terms or words used in the present specification and claims should be interpreted as meaning and concept conforming to the technical spirit of the present invention.
- [28] Throughout the specification, when a part "includes" a certain component, this means that other components may be further included instead of being excluded, unless specifically stated to the contrary.
- [29] In addition, when one component is said to be "connected", "transmitted", "sent", "received", or "transferred" to other component, this includes not only the case where one component is directly connected, transmitted, sent, received, or transferred to another component, as well as the case where one component is indirectly connected, transmitted, sent, received, or transferred to another component with still another component in between.
- [30] In addition, terms such as "part", "module", and "device" described in the specification mean a unit that processes at least one function or operation, and may be implemented as hardware, software, or a combination of hardware and software.
- [31] Hereinafter, embodiments of the present invention will be described in detail with reference to the accompanying drawings.
- [32] FIG. 1 is a diagram showing the configuration of a blockchain search system according to an embodiment of the present invention.
- [33] Referring to FIG. 1, the blockchain search system includes multiple blockchain networks 1, a blockchain search server 2, and a user terminal 3.
- [34] The multiple blockchain networks 1 include blockchain networks 1-1, 1-2, and 1-3 operated by different operating entities. Each of the blockchain networks 1-1, 1-2, and 1-3 includes a plurality of nodes N, in which a block is stored in each node N.
- [35] The blockchain search server 2 receives a search term for identifying a block, from the user terminal 3; when selecting a blockchain network to be searched from among the multiple blockchain networks, enters the search term by accessing the selected blockchain network, in order to search the selected blockchain network for the block corresponding to the search term; receives data stored in the found block from the selected blockchain network; and transmits the received data to the user terminal.
- [36] When a user enters a search term for identifying a block, and selects a blockchain network to be searched from among the multiple blockchain networks, the user terminal 3 transmits the entered search term and the selected blockchain network to the blockchain search server 2.
- [37] The user terminal 3 may be, for example, a mobile phone, a computer, or a laptop,

and program or application in which a blockchain data search method according to an embodiment of the present invention is implemented may be installed and executed.

- [38] According to an embodiment, the search term may be any one of a hash value, a key value, and a QR code value.
- [39] The search term will be described with reference to FIGS. 2 to 3.
- [40] FIG. 2 is a diagram showing an example of a structure of a block generated at a node N of FIG. 1.
- [41] Referring to FIG. 2, the block 100 is divided into a block head 200 and a block body 300. In the block head 200, previous block hash, Merkle hash root, timestamp, Bits, and Nonce are stored.
- [42] The previous block hash is a hash value obtained by hashing the previous block header using a hash function. In the case of a bitcoin, a hash value obtained by hashing the previous block header twice using a SHA-256 hash function, that is, a value of SHA-256(SHA-256(previous block header)) is stored.
- [43] The Merkle hash root is a hash value located at the root of the tree when configuring the transaction hash of the transaction information included in the current block in the form of a binary tree.
- [44] The timestamp represents a creation time of the block.
- [45] The Bits represents the difficulty target for a proof-of-work algorithm of the block.
- [46] The Nonce is a counter for finding a value lower than a specific target value.
- [47] In this embodiment, since a block is specified by the previous block hash, the hash value may be used as a search term.
- [48] FIG. 3 is a diagram showing an example of a structure of a block generated at a node N of FIG. 1.
- [49] Referring to FIG. 3, a block may include a block number, number of transmission times, and transmission contents. According to the embodiment, the block number is numbered so that a value thereof is sequentially increased as blocks are generated. Accordingly, the block number may be used as a search term.
- [50] Depending on the embodiment, the search term entered from the user terminal 3 may be in the form of a QR code.
- [51] The user terminal 3 may scan the QR code, convert it into the search term corresponding to the QR code, and transmit information about the converted search term to the blockchain search server 2.
- [52] Herein, the user terminal 3 may be a mobile phone having a QR code scanner function or may be used in connection with a separate QR code scanner.
- [53] Since the above-mentioned hash value or block number is long in length and complicated, the user may enter the same incorrectly. Meanwhile, since the search term may be entered in a simple way through a QR code scanner when entering the search

term in the form of a QR code, there is an advantage of excellent usability.

[54] FIG. 4 is a flowchart showing a blockchain search method according to an embodiment of the present invention.

[55] Referring to FIG. 4, the blockchain search method according to an embodiment of the present invention includes receiving a search term for identifying a block from a user terminal, and selecting a blockchain network to be searched from among multiple blockchain networks (S100); receiving a private key from the user terminal and releasing the security of the selected blockchain network using the received private key and public key (S200); searching the selected blockchain network for a block corresponding to the search term by accessing the selected blockchain network and entering the search term (S300); receiving data stored in the found block from the selected blockchain network and transmitting the received data to the user terminal (S400).

[56] First, a user enters a search term for identifying a block into the user terminal 3, and selects a blockchain network to be searched from among multiple blockchain networks (S100).

[57] The search term is a value capable of identifying a block, such as a hash value or a block number of the block. In addition, the search term may be input in the form of a QR code as well as text.

[58] The multiple blockchain networks may be operated on different operating entities, such as Facebook's Libra, Kakao's Clayton, and NaverLine's Link.

[59] Step S100 may include receiving the search term from the user terminal and providing the user terminal with blockchain network candidates in which a block is capable of being searched for using the search term on the basis of a type of the search term; and selecting one from among the blockchain network candidates as the blockchain network by the user terminal.

[60] The type of the search term may be, for example, the length of input text. For example, when a blockchain network A uses a hash value represented by 12 characters of text, and a blockchain network B uses a block number represented by 10 characters of text, the blockchain network A or the blockchain network B may be provided as the blockchain network candidate based on the length of the input text.

[61] Next, the blockchain search server 2 receives a private key from the user terminal, and releases the security of the selected blockchain network using the received private key and public key (S200).

[62] Blocks in the blockchain network may be encrypted using the private key and the public key. Accordingly, the blockchain search server 2 receives the private key and public key from the user terminal 3, and release the security of the selected blockchain network using the received private key and public key.

[63] Next, the blockchain search server 2 accesses the selected blockchain network and

inputs the search term, so that the block corresponding to the search term is searched for in selected blockchain network (S300).

- [64] Each blockchain network 1-1, 1-2, 1-3 constituting the multiple blockchain networks 1 may include a search server (not shown) that searches for a block corresponding to the search term. The blockchain search server 2 may input the search term in the search server of the selected blockchain network, to cause a block corresponding to the search term to be searched for by the search server of the selected blockchain network.
- [65] Next, the blockchain search server 2 receives data stored in the searched block from the selected blockchain network and transmits the received data to the user terminal (S400).
- [66] According to an embodiment, when the data stored in the found block is a URL link, the blockchain search server 2 may access a specific data storage server corresponding to the URL link to transmit data received from the specific data storage server to the user terminal 3. Herein, the received data may be an image or a video.
- [67] In the case of an image or a video file, each node of the blockchain network 1 may store the same directly in the block. However, because the image or video file has a large capacity, it may be stored on other data storage servers, and only a location of the data storage server where the image or video files are stored may be stored in the block.
- [68] According to this embodiment, when the location of the data storage server is stored in the found block, the blockchain search server 2 does not transmit the location of the data storage server to the user terminal 3 as it is, but directly access the data storage server to receive the image or video file and transmit the received image or video file to the user terminal 3.
- [69] According to an embodiment, when data stored in the found block indicates a specific service, the blockchain search server 2 may execute the client of a specific service and transmit the received data to the user terminal 3. The specific service may be any one of a messenger service, a news service, a music service, and a game.
- [70] According to this embodiment, the data stored in the block may represent a specific service, and herein, the blockchain search server 2 can execute a specific service using the web or application. Accordingly, when data is transmitted from a server providing the specific service, the data may be transferred to the user terminal 3. According to this embodiment, a user can be provided with a service by searching a blockchain network for a block without having to execute a separate service.
- [71] FIGS. 5a, 5b and 5c are diagrams showing a screen of a user terminal in which a blockchain search method is implemented according to an embodiment of the present invention.
- [72] As shown in FIG. 5a, a screen of a user terminal 3 is provided with a search term

input window 310, a blockchain network input window 320, and blockchain network candidates 330.

- [73] Accordingly, the user enters a search term such as a hash value or a block number into the search term input window 310. The user may directly enter a name of the blockchain network into the blockchain network input window 320, or select any one from among the blockchain network candidates 330.
- [74] A view in FIG. 5b is a screen showing a state in which a search term and a blockchain network are input, followed by the screen of FIG. 5a.
- [75] A view in FIG. 5c is a screen showing a search result, followed by the screen of FIG. 5b.
- [76] In the blockchain network entered into the blockchain network input window 320, the data stored in the block found using the search term, which is entered into the search term input window 310, appears in a search result window 340 of FIG. 5c. Herein, the data stored in the block may be a text.
- [77] FIG. 6 is a diagram showing a screen of a user terminal in which a blockchain search method is implemented according to an embodiment of the present invention, which is a screen showing other search results.
- [78] In FIG. 6, the data stored in the block is a URL link, and the blockchain search server 2 may access a specific data storage server corresponding to the URL link to receive an image file and transmit the same to the user terminal 3. Accordingly, an image is displayed in the search result window of the user terminal 3, so that the user can directly check the image from the user terminal 3.
- [79] FIG. 7 is a diagram showing a screen of a user terminal in which a blockchain search method is implemented according to an embodiment of the present invention, which is a screen showing other search results.
- [80] In FIG. 7, the data stored in the block is a URL link, and the blockchain search server 2 may access a specific data storage server corresponding to the URL link to receive a video file and transmit the same to the user terminal 3. Accordingly, the video is displayed in the search result window of the user terminal 3, and the user may play the video directly from the user terminal 3.
- [81] FIG. 8 is a diagram illustrating a screen of a user terminal in which a blockchain search method is implemented according to an embodiment of the present invention, which is a screen showing other search results.
- [82] The data stored in the block in FIG. 8 represents a news providing service, and the blockchain search server 2 may access a server providing the news providing service to transmit the received file to the user terminal 3. Accordingly, a screen provided by the news providing service appears in the search result window of the user terminal 3, in which some images of news and some website addresses for news may be displayed,

as illustrated in FIG. 8.

- [83] The present invention has been described in detail through preferred embodiments, but the present invention is not limited thereto. It is apparent to those skilled in the art that various modifications and applications can be made without departing from the spirit of the present invention. Therefore, it should be interpreted that the true protection scope of the present invention should be interpreted by the following claims, and all technical ideas within the equivalent scope are included in the scope of the present invention.