

BLOCKCHAIN-BASED MONITORING DATA PROCESSING METHOD AND DEVICE, EQUIPMENT AND MEDIUM

TECHNICAL FIELD

[0001] The present disclosure herein relates to the field of computer technology, and in particular to a blockchain-based monitoring data processing method and device, equipment and medium.

BACKGROUND

[0002] The monitoring system is an important part of the security system. Cameras and sensors collect data, analyze the collected information, and store the analyzed monitoring information.

[0003] Generally, when querying monitoring information, you only need correct login information to query monitoring information on multiple different terminal equipment. That is, enter the login account and password on the terminal equipment. After verifying that the account number and password are correct, the terminal equipment can read the monitoring information repository and query the relevant monitoring information. However, when the account and password are stolen, the relevant monitoring information can still be queried. It can be seen that there is a large risk of leakage of monitoring information in related technologies.

[0004] Therefore, how to reduce the risk of monitoring information leakage is an urgent problem that those skilled in the art need to solve.

SUMMARY

[0005] In order to reduce the risk of monitoring information leakage, the present disclosure provides a blockchain-based monitoring data processing method and device, equipment and medium.

[0006] In the first aspect, the present disclosure provides a blockchain-based monitoring data processing method, adopting the following technical solution:

a blockchain-based monitoring data processing method, comprising:

obtaining a monitoring information and a first identity identifier corresponding to a monitoring equipment, wherein the monitoring information is information obtained based on the analysis of monitoring images collected by the monitoring equipment, wherein the monitoring information comprises monitoring images and corresponding analysis results, and the monitoring images are human images or environmental

change images;

determining a plurality of second identity identifiers corresponding to the first identity identifier based on the first identity identifier, wherein the second identity identifier is an identity identifier of a terminal equipment with access permission corresponding to the first identity identifier;

establishing an associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers; and

encrypting the associated information to obtain an encrypted associated information; and uploading the monitoring information and the encrypted associated information to a blockchain node.

[0007] In a possible implementation method, wherein the monitoring information at least comprises: a text information, and determining the plurality of second identity identifiers corresponding to the first identity identifier based on the first identity identifier, comprising:

obtaining a network information corresponding to the first identity identifier;

determining a plurality of to-be-determined equipment using the same network corresponding to the first identity identifier based on the network information;

obtaining an access history information corresponding to each of the plurality of to-be-determined equipment;

performing information category identification on the text information to determine the information category of the monitoring information;

selecting a plurality of target equipment whose reference information categories are the same as the categories to which the information belongs from the plurality of to-be-determined equipment, wherein the reference information categories are obtained by identifying the historical reference information; and

obtaining an equipment identifier corresponding to each of the plurality of target equipment, and determining the equipment identifier corresponding to each of the plurality of target equipment to be the plurality of second identity identifiers corresponding to the first identity identifier.

[0008] In a possible implementation method, encrypting the associated information to obtain the encrypted associated information comprises:

obtaining a location information of the monitoring equipment, and determining a privacy level corresponding to an installation location information for the monitoring equipment based on a preset corresponding relationship between the location

information and the privacy level and the installation location information for the monitoring equipment;

determining a target information encryption policy based on the privacy level and a preset information encryption strategy; and

encrypting the associated information using the target information encryption policy to obtain the encrypted associated information.

[0009] In a possible implementation method, obtaining the monitoring information comprises:

obtaining multiple consecutive monitoring images within a preset time period;

determining whether there is an image change based on the multiple consecutive monitoring images;

if so, performing image recognition on a changed image to determine a category of the changed image, and the category of the changed image comprises: a personnel change, and/or an environmental change;

if the category of the changed image is the personnel change, determining a personnel identification information based on the changed image, and the personnel identification information at least includes a personnel identity identifier and a personnel action event;

if the category of the changed image is the environmental change, obtaining an environmental change data, and determining an environmental safety risk assessment information based on the environmental change data; and

determining the multiple consecutive monitoring images and an image change information as the monitoring information, and the image change information comprises: the personnel identification information and/or the environmental safety risk assessment information.

[0010] In a possible implementation method, uploading the monitoring information and the encrypted associated information to the blockchain node comprises:

obtaining a data carrying capacity information corresponding to each of the all blockchain nodes;

determining a target blockchain node that is not less than an expected carrying capacity information from all blockchain nodes based on the corresponding data carrying capacity information and expected carrying capacity information of all blockchain nodes, and the expected carrying capacity information is determined based on the monitoring information and the encrypted associated information; and

uploading the monitoring information and the encrypted associated information to the target blockchain node.

[0011] In a possible implementation method, after uploading the monitoring information and the encrypted associated information to the blockchain node, further comprising:

obtaining a reward corresponding to the expected carrying capacity information based on the expected carrying capacity information, and sending the reward to the target blockchain node, wherein the target blockchain node is the blockchain node that uploads the monitoring information and the encrypted associated information.

[0012] In a possible implementation method, before establishing the associated information between the monitoring information, the first identity identifier and the plurality of second identity identifiers, further comprising:

obtaining an information format corresponding to the monitoring information, and determining whether the information format is a preset standard format;

if not, converting the information format corresponding to the monitoring information into the preset standard format to obtain a format-converted monitoring information;

correspondingly, establishing the associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers, comprising:

establishing an associated information between the format-converted monitoring information, the first identity identifier, and the plurality of second identity identifiers.

[0013] In the second aspect, the present disclosure provides a blockchain-based monitoring data processing device, adopting the following technical solution:

a blockchain-based monitoring data processing device, comprising:

an acquisition module, wherein the acquisition module is used for obtaining a monitoring information and a first identity identifier corresponding to a monitoring equipment, wherein the monitoring information is information obtained based on the analysis of monitoring images collected by the monitoring equipment, wherein the monitoring information comprises monitoring images and corresponding analysis results, and the monitoring images are human images or environmental change images;

a second identity identifier determination module, wherein the second identity identifier determination module is used for determining a plurality of second identity

identifiers corresponding to the first identity identifier based on the first identity identifier, wherein the second identity identifier is an identity identifier of a terminal equipment with access permission corresponding to the first identity identifier;

an associated information establishing module, wherein the associated information establishing module is used for establishing an associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers; and

a storage module, wherein the storage module is used for encrypting the associated information to obtain an encrypted associated information; and uploading the monitoring information and the encrypted associated information to a blockchain node.

[0014] In the third aspect, the present disclosure provides an electronic equipment, adopting the following technical solution:

at least one processor;

a memory; and

at least one application program, wherein at least one application program is stored in the memory and configured to be executed by at least one processor, the at least one application program is configured to: execute the blockchain-based monitoring data processing method as described in any one of the first aspect.

[0015] In the fourth aspect, the present disclosure provides a computer-readable storage medium, adopting the following technical solution:

a computer-readable storage medium, wherein a computer program is stored thereon, and when the computer program is executed in a computer, the computer is executed the blockchain-based monitoring data processing method as described in any one of the first aspect.

[0016] In summary, the present disclosure includes the following beneficial technical effects:

obtaining a monitoring information and a first identity identifier corresponding to a monitoring equipment, and then determining a plurality of corresponding second identity identifiers based on the first identity identifier, so as to determine the access permission for the monitoring information and prevent the identity identifier of the terminal equipment beyond the access permission from obtaining the monitoring information to reduce the probability of the monitoring information being leaked; then associating the monitoring information, the first identity identifier and the second

identity identifier and encrypting them to prevent the second identity identifier information with access permission from being tampered with, and then storing the encrypted associated information in the blockchain nodes with good data confidentiality. By constructing the association relationship between the monitoring information, the first identity identifier and the second identity identifier, encrypting it and uploading it to the blockchain, then when reading the monitoring data, only if the identity identifier is any second identity identifier, can we get the monitoring data to be queried. Compared with the prior art, according to the present disclosure, the protection of monitoring information is enhanced by encrypting the monitoring information, the first identity identifier and a plurality of second identity identifiers and then uploading them to the blockchain, and the technical issue of high risk of monitoring information leakage in the prior art is resolved.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] FIG. 1 is a schematic diagram of a blockchain-based node connection provided by an embodiment of the present disclosure.

[0018] FIG. 2 is a flow chart diagram of a blockchain-based monitoring data processing method provided by an embodiment of the present disclosure.

[0019] FIG. 3 is a structure schematic diagram of a blockchain-based monitoring data processing device provided by an embodiment of the present disclosure.

[0020] FIG. 4 is a structure schematic diagram of an electronic equipment provided by an embodiment of the present disclosure.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0021] The present disclosure will be further described in detail below with reference to FIG. 1 to 4.

[0022] This specific embodiment is only an explanation of the present disclosure, and it is not a limitation of the present disclosure. Those skilled in the art can make modifications to this embodiment without creative contribution as needed after reading this specification, but are protected by patent law as long as they are within the scope of the present disclosure.

[0023] In order to make the object, technical solutions and advantages of the embodiments of the present disclosure clearer, the technical solutions in the embodiments of the present disclosure will be clearly and completely described below in conjunction with the accompanying drawings in the embodiments of the present disclosure. Obviously, the described embodiments are part of the embodiments of the

present disclosure, but not all of them. Based on the embodiments in the present disclosure, all other embodiments obtained by those of ordinary skilled in the art without creative efforts fall within the scope of protection of the present disclosure.

[0024] In addition, the term "and/or" in the present disclosure is only a description of the association relationship between related objects, indicating that there can be three types of relationships, for example, A and/or B, which can indicate the presence of A alone, the presence of A and B simultaneously, and the presence of B alone. In addition, the character "/" in the present disclosure, unless otherwise specified, generally indicates that the related objects are in an "or" relationship.

[0025] To facilitate understanding, the following technical terms are explained.

[0026] Blockchain: blockchain is a new application model of computer technology such as distributed data storage, peer-to-peer transmission, consensus mechanism, encryption algorithm and so on. Blockchain is essentially a decentralized database. It is a series of data blocks generated using cryptographic algorithm. Each data block contains a batch of network transaction information and is used to verify validity of information (anti-counterfeiting) and generate the next block. Blockchain can include the blockchain underlying platform, the platform product service layer and the application service layer.

[0027] In the embodiment of the present disclosure, blockchain refers to a blockchain network. Each blockchain network contains multiple blockchain nodes. When the monitoring information and encrypted associated information are successfully uploaded to any blockchain node, the monitoring information and the encrypted associated information will be quickly transferred to other blockchain nodes for storage within a second-level time period, and each blockchain node will cooperate with each other. As shown in FIG. 1, it is a schematic diagram of a blockchain node connection provided by an embodiment of the present disclosure.

[0028] In addition, each blockchain node corresponds to a node identification, and each blockchain node in the blockchain network can store the node identifications of other blockchain nodes in the data sharing system, so that the generated blocks can be broadcasted to other blockchain nodes based on the node identifications of other blockchain nodes in the future. The node identification can be an IP (Internet Protocol, a protocol for interconnection between networks) address and any other information that can be used to identify the node.

[0029] The embodiment of the present disclosure provides a blockchain-based

monitoring data processing method, which is executed by an electronic equipment. The electronic equipment can be a server, which can be an independent physical server, a server cluster or a distributed system comprising multiple physical servers, or a cloud server providing cloud computing services. The server can be connected directly or indirectly through wired or wireless communication methods, which is not limited in the embodiments of the present disclosure. The embodiments of the present disclosure do not limit the applicable scenarios for blockchain-based monitoring data processing, and can be applied to enterprise scenarios.

[0030] Combined with FIG. 2, FIG. 2 is a flow chart diagram of a blockchain-based monitoring data processing method provided by an embodiment of the present disclosure. The method comprises Step 101, Step 102, Step 103 and Step 104, wherein:

Step 101: obtaining a monitoring information and a first identity identifier corresponding to a monitoring equipment, wherein the monitoring information is information obtained based on the analysis of monitoring images collected by the monitoring equipment, wherein the monitoring information comprises monitoring images and corresponding analysis results, and the monitoring image is either an image of a person or an image of environmental changes.

[0031] Specifically, after receiving a data processing request, the monitoring data processing procedure can be executed, and the electronic equipment being pre-integrated with a monitoring program that oversees the triggering behavior of the processing request. Once the processing request is detected to be triggered, the monitoring program and the first identity identifier of the monitoring equipment are obtained.

[0032] The monitoring information comprises monitoring images and corresponding analysis results. The monitoring image may be an image of a person, or may be an image corresponding to an environmental change, wherein the environmental change may be: a change in the position of a document indoors. Different types of monitoring images require different analysis methods. For example, when the monitoring image type is an image of a person, the analysis methods include personnel change analysis and the identity identification of the changed personnel; and when the monitoring image type is an image of the environment, the analysis methods include: environmental change analysis and environmental risk assessment analysis.

[0033] In the embodiment of the present disclosure, the first identity identifier

corresponding to the monitoring equipment can be the factory number of the monitoring equipment, or it can be an artificially set monitoring number, for example, monitoring equipment No. 001, monitoring equipment No. 020, or monitoring equipment No. 013, each monitoring equipment corresponds to a different first identity identifier, and all are stored by a person skilled into the electronic equipment.

[0034] Step 102: determining a plurality of second identity identifiers corresponding to the first identity identifier based on the first identity identifier, wherein the second identity identifier is an identity identifier of a terminal equipment with access permission corresponding to the first identity identifier.

[0035] Specifically, the terminal equipment with access permission is determined to implement restrictions on the terminal equipment with access permission and prevent equipment without access permission from accessing the monitoring information, effectively reducing the risk of leakage of the monitoring information.

[0036] In the embodiment of the present disclosure, in order to improve the accuracy of confirming the terminal equipment with access permission, the second identity identifier can be the factory number corresponding to the terminal equipment with access permission, or it can be the location of the terminal equipment with access permission, for example, the first terminal equipment with access permission in the finance office and the second terminal equipment with access permission in the finance office. The embodiment of the present disclosure does not limit the specific content of the second identity identifier.

[0037] Step 103: establishing an associated information between the monitoring information, the first identity identifier and the plurality of second identity identifiers.

[0038] Specifically, the establishment of the association relationship can be achieved in the form of a work list, which stores the monitoring information, the first identity identifier, and the second identity identifier. By establishing the association relationship, the identity of the terminal equipment with access permission to access the aforementioned monitoring equipment can be clarified, while preventing the terminal equipment without access permission from querying the mentioned monitoring information. It is understandable that the storage location of the associated information is a blockchain network, which means that once the aforementioned associated information is uploaded to the blockchain, the monitoring information, the first identity identifier, and the several second identity identifiers become tamper-proof. When subsequently accessing the monitoring information, it can be

directly determined whether the monitoring information can be accessed based on the second identity identifiers stored in the blockchain network. As shown in Table 1, it is a schematic table of associated information provided by the embodiment of the present disclosure, taking the monitoring equipment of the finance office in the enterprise as an example.

[0039] Table 1

Monitoring information	First identity identifier	Second identity identifier
	No. 013	The first access equipment in the finance office
		The second access equipment in the finance office
		The second access equipment in the finance office

[0040] Step 104: encrypting the associated information to obtain an encrypted associated information; and uploading the monitoring information and the encrypted associated information to a blockchain node.

[0041] Specifically, in this embodiment of the present disclosure, the associated information may be encrypted using asymmetric encryption or privacy-level encryption. Preferably, the associated information is encrypted using privacy-level encryption, which can encrypt the monitoring information in a targeted manner, and setting stronger encryption for data with higher importance can effectively improve the encryption of important encrypted information. The protection strength of the blockchain network itself is tamper-proof and highly confidential, so uploading it to the blockchain node can effectively improve the protection of monitoring information and encrypted associated information, and reduce the risk of monitoring information being leaked. Subsequently, the blockchain network can send the newly generated blocks to other blockchain nodes, the other blockchain nodes will verify the newly generated blocks, and after completing the verification, the newly generated blocks will be added to the blockchain where it is stored to complete the storage of monitoring information and encrypted associated information. The embodiment of the present disclosure does not limit the specific verification method for input information, and users can set it themselves.

[0042] Based on the above embodiment, obtaining a monitoring information and a first identity identifier corresponding to a monitoring equipment, and then determining a plurality of corresponding second identity identifiers based on the first identity identifier, so as to determine the access permission for the monitoring information and prevent the identity identifier of the terminal equipment beyond the access permission from obtaining the monitoring information to reduce the probability of the monitoring information being leaked; then associating the monitoring information, the first identity identifier and the second identity identifier and encrypting them to prevent the second identity identifier information with access permission from being tampered with, and then storing the encrypted associated information in the blockchain nodes with good data confidentiality. By constructing the association relationship between the monitoring information, the first identity identifier and the second identity identifier, encrypting it and uploading it to the blockchain, then when reading the monitoring data, only if the identity identifier is any second identity identifier, can we get the monitoring data to be queried. Compared with the prior art, according to the present disclosure, the protection of monitoring information is enhanced by encrypting the monitoring information, the first identity identifier and a plurality of second identity identifiers and then uploading them to the blockchain, and the technical issue of high risk of monitoring information leakage in the prior art is resolved.

[0043] Furthermore, when an equipment needs to access monitoring information from the blockchain network, the access equipment sends an access request, which includes the monitoring information to be accessed and the identity identifier of the access equipment, and the electronic equipment sends the access request to the blockchain network, after receiving the access request, the electronic equipment retrieves the associated information corresponding to the access request from the blockchain network, and matches the identity identifier of the access equipment with the second identity identifier in the associated information one by one to determine whether the access equipment has access permission, if any second identity identifier in the associated information is the same as the identity identifier of the access equipment, it can be determined that the access equipment has access permission, and the monitoring information in the associated information will be sent to the access equipment; otherwise, it is determined that the access equipment does not have access permission, and a reminder signal for rejecting the access is generated.

[0044] Furthermore, in the embodiment of the present disclosure, in order to accurately determine the second identity identifier, the monitoring information at least comprises: a text information. Step 102, determining a plurality of second identity identifiers corresponding to the first identity identifier based on the first identity identifier, including the Step 102A to Step 102F (not shown in the figures), wherein:

Step 102A: obtaining a network information corresponding to the first identity identifier.

[0045] Specifically, the network information may be a network code or network identifier corresponding to the wireless network or wired network used by the monitoring equipment.

[0046] Step 102B: determining a plurality of to-be-determined equipment using the same network corresponding to the first identity identifier based on the network information.

[0047] Specifically, the electronic equipment can identify equipment other than the monitoring equipment that are using the network, that is, to-be-determined equipment, by searching the network addresses of all equipment within a preset location range. The embodiment of the present disclosure does not limit the preset location range, which can be input into the electronic equipment in advance by technicians. It can be understood that when the monitoring equipment is installed in an enterprise, the preset location range at least covers the floor where the enterprise is located, and thus can identify a plurality of to-be-determined equipment that use the same network as the monitoring equipment.

[0048] Step 102C: obtaining an access history information corresponding to each of the plurality of to-be-determined equipment.

[0049] Specifically, the access history information can be the information input when reviewing the monitoring. For example, when the need arises to query the monitoring from the finance office on January 3, 2022. Each time the equipment performs a query operation, the query content information will be automatically uploaded to the electronic equipment.

[0050] Step 102D: performing information category identification on the text information to determine the information category of the monitoring information.

[0051] Specifically, a classification tree can be used to identify key fields in the text information to determine the information category. For example, given the text information "The location of financial document No. 01 has been moved on May 15,

2023,” the key field "financial document" can be input into a preset classification tree to determine the information category as the financial category. The classification tree is obtained based on multiple training key fields and their corresponding category labels. The embodiment of the present disclosure does not limit the training process of the classification tree, and users can set it themselves.

[0052] Step 102E: selecting a plurality of target equipment from the plurality of to-be-determined equipment, whose accessing information categories match the categories of the information, wherein the accessing information categories are obtained through identifying the access history information.

[0053] Step 102F: obtaining an equipment identifier corresponding to each of the plurality of target equipment, and determining the equipment identifier corresponding to each of the plurality of target equipment as the plurality of second identity identifiers corresponding to the first identity identifier.

[0054] Specifically, the electronic equipment identifies the key fields in the access history information, and the identification process is the same as Step 102D, which will not be repeated in the embodiments of the present disclosure. Thereby, it determines a plurality of accessing information categories, and matches each accessing information category with the corresponding information category to identify the target equipment; obtaining the equipment identifier corresponding to the target equipment, and determining the equipment identifier corresponding to the target equipment as the plurality of second identity identifiers corresponding to the first identity identifier.

[0055] Based on the above embodiment, obtaining a network information corresponding to the first identity identifier. Generally, in order to improve the network protection, the monitoring equipment and the access equipment are set up to use the same network. Therefore, multiple to-be-determined equipment can be accurately determined based on the network information; obtaining the access history information, performing information identification on the text information to determine the category of the information, and then selecting from multiple to-be-determined equipment a plurality of target equipment whose information category is the same as the category to which the information belongs, in order to obtain several accurate target equipment; and then obtaining the device identification of the target equipment, and determining the target equipment identification as the second identity identifier, effectively improving the accuracy of determining the

second identity identifier.

[0056] Furthermore, in the embodiment of the present disclosure, Step 104 encrypts the associated information to obtain encrypted associated information, including Step A1 - Step A3 (not shown in the figures), wherein:

Step A1: obtaining a location information of the monitoring equipment, and determining a privacy level corresponding to an installation location information for the monitoring equipment based on a preset corresponding relationship between the location information and the privacy level and the installation location information for the monitoring equipment.

[0057] Specifically, the location information of the monitoring equipment is input into the electronic equipment in advance. In the embodiment of the present disclosure, the privacy level can be divided into the first level and the second level; different installation locations of the monitoring equipment correspond to different privacy levels of the monitoring information. For example, when the installation location of the monitoring equipment is the financial room of an enterprise, then the corresponding privacy level can be the first level. When the monitoring equipment is installed in a public area of the enterprise, the corresponding privacy level can be the second level. The monitoring information corresponding to the first level is more important than that corresponding to the second level. The corresponding relationship between the preset installation location of the monitoring equipment and the privacy level is stored in the electronic equipment by the technician in advance, so that the privacy level can be determined. It is understandable that by classifying the privacy levels of the monitoring information, the monitoring information can be processed in a targeted manner and precise processing of the monitoring information can be achieved.

[0058] Step A2: determining a target information encryption policy based on the privacy level and a preset information encryption policy.

[0059] Step A3: encrypting the associated information using the target information encryption policy to obtain the encrypted associated information.

[0060] Specifically, the preset information encryption policy can be input into the electronic equipment in advance by technicians. The preset information encryption policy can specifically include: when the privacy level is the first level, the corresponding information encryption policy performs two hash operations. By performing two hash operations, it can not only increase the length of the hash value,

but also enhance the internal complexity of the hash, which can further effectively improve the resistance to attacks and prevent the leakage of the monitoring information. In the embodiment of the present disclosure, it is preferred to use Secure Hash Algorithm 3 (SHA-3) to perform hash operations. Compared with Secure Hash Algorithm 0 (SHA-0) and Secure Hash Algorithm 2 (SHA-2), the algorithm mechanism of SHA-3 differs significantly. During the operation process, SHA-3 can input and output data through random permutation and combination. The embodiment of the present disclosure does not limit the specific process of hash operation using SHA-3; when the privacy level data is the second level, a hash operation is performed on the associated information to obtain the encrypted associated information.

[0061] Furthermore, in a practical implementation, Step A3 can be executed for each received associated information to effectively improve the efficiency of associated information processing. Alternatively, it is also possible to perform Step A3 only for the associated information received after a preset number of iterations. It can be understood that the privacy level corresponding to the associated information received after a preset number of iterations is the same. In other words, after receiving associated information with the same privacy level for a preset number of iterations, it is encrypted to obtain the encrypted associated information, thus effectively reducing the calculation amount for associated information. The embodiment of the present disclosure does not limit the preset number of iterations.

[0062] Based on the above embodiments, the privacy level corresponding to the installation location information of the monitoring equipment is determined based on both the installation location information and the privacy level of the monitoring equipment. Then, the target information encryption policy is determined based on the privacy level and a preset information encryption policy, in order to perform corresponding encryption processing in accordance with the importance of the monitoring information. The importance of monitoring information varies across different scene categories. By determining the privacy level, the monitoring information can be processed in a targeted manner, and the higher the importance of the privacy data, the higher the corresponding encryption strength, which effectively improves the protection of encrypted information and reduces the risk of leakage.

[0063] Furthermore, in the embodiment of the present disclosure, obtaining the monitoring information comprises Step B1 to Step B6 (not shown in the figures), wherein:

[0064] Step B1: obtaining multiple consecutive monitoring images within a preset duration.

[0065] Specifically, when the electronic equipment detects the monitoring information processing request, the monitoring image is obtained from the monitoring equipment. The embodiment of the present disclosure does not limit the preset duration, which may be the default duration set by the monitoring equipment, or may be the default duration modified by the user. It can be understood that the multiple consecutive monitoring images may be multiple frames of consecutive monitoring images corresponding to the monitoring video.

[0066] Step B2: determining whether there is an image change based on the multiple consecutive monitoring images.

[0067] Step B3: if so, performing image recognition on a changed image to determine a category of the changed image, and the category of the changed image comprises: a personnel change, and/or an environmental change.

[0068] Specifically, regarding the same image, it may be determined whether there is an image change based on the comparison between the start image and the end image of a plurality of consecutive monitoring images, or whether there is a change in the position of any object based on the comparison of any two consecutive images. If such changes are detected, Step B3 is performed to identify the changed image and determine the category it belongs to, where the changed image may include at least two of the monitoring images. The electronic equipment extracts images with changes and identifies them based on the extracted images to determine whether there are changes in personnel and/or changes in the environment. It can be understood that when there are changes in the position and limbs of personnel in the monitoring image, such changes can be identified as personnel changes; environmental changes can refer to changes in the location of a document.

[0069] Step B4: if the category of the changed image is the personnel change, determining a personnel identification information based on the changed image, and the personnel identification information at least includes a personnel identity identifier and a personnel action event.

[0070] Specifically, when the category of the changed image is the personnel change, the change image is a selected image of personnel with limb changes from multiple consecutive monitoring images. The personnel identification information may be determined through face recognition, by extracting personnel face image and

recognizing it to identify the personnel identity identifier. The personnel face image and the corresponding personnel identity identifier are pre-inputted into an electronic equipment. Based on a plurality of personnel change images, the moving limb of the personnel is determined, and the change trajectory of the moving limb is recognized to determine the moving information, which constitutes the personnel action event. For example, using facial recognition and analysis of changes in moving limbs, we can determine the corresponding personnel identification information. Specifically, Zhang San is eating, while Li Si and Wang Wu are talking.

[0071] Furthermore, the personnel identity identifier can be used to determine whether the person is a legal occupant. For example, when a certain room is targeted, it is determined whether the personnel identity identifier corresponds to the preset compliant personnel identity identifier. If so, it is determined that there is no risk; otherwise, it is determined that there is a risk and an early warning is issued. The preset compliant personnel identity identifier can be artificially set according to the scene; when targeting a public place, it is judged whether the personnel identity identifier corresponds to the identity identifier of dangerous persons. If so, the risk is identified and an early warning is issued. The identity identifier of the dangerous person is determined based on the police database or security database. The database can be a network database and can update the corresponding data of criminals and suspects in real time.

[0072] Step B5: if the category of the changed image is the environmental change, obtaining an environmental change data, and determining an environmental safety risk assessment information based on the environmental change data.

[0073] Specifically, when the category of the changed image belongs to environmental change, for example, when the location of a document in the finance room is changed, the corresponding environmental change data would be the difference in location between the first location before the document's location change and the second location after the change. It is then judged whether the location difference is not greater than a preset location difference threshold. If so, the corresponding environmental safety risk assessment information can be: the document is within a safe location range; otherwise, the corresponding environmental safety risk assessment information is: the document is in a dangerous location range. The three-dimensional coordinates of the financial room can be established through monitoring images to obtain the first position and the second position of the document;

the embodiment of the present disclosure does not limit the preset position difference threshold. One can understand that the protection measures for documents are relatively strict, and even documents need to be consulted within the prescribed scope. For example, financial office documents are only allowed to be reviewed in the financial room and are not allowed to be taken out of the financial room for review.

[0074] Step B6: determining the multiple consecutive monitoring images and an image change information as the monitoring information, and the image change information comprises: the personnel identification information and/or the environmental safety risk assessment information.

[0075] Specifically, the image change information can be converted into text content corresponding to the monitoring image, so that the above text content and the corresponding monitoring image are determined as monitoring information.

[0076] Based on the above embodiments, multiple consecutive monitoring images are obtained within a preset duration to determine whether there is any image change. If so, image recognition is performed to determine the category of the changed image, in order to accurately record image change information; when the category of the change image belongs to personnel change, personnel identity identifier and personnel action events are determined based on the personnel change image to accurately record the personnel change information; if the category of the change image belongs to environmental change, the environmental change data is determined based on the environmental change image. The environmental change data is then input into the environmental safety risk assessment model to obtain environmental safety risk assessment information, thus accurately recording the current environmental safety risk. Subsequently, the multiple consecutive monitoring images and image change information are identified as monitoring information, effectively improving the accuracy of monitoring information recording.

[0077] Furthermore, in the embodiment of the present disclosure, Step 104 uploads the monitoring information and the encrypted associated information to the blockchain node, including Step C1 to Step C3 (not shown in the figure), wherein:

[0078] Step C1: obtaining a data carrying capacity information corresponding to each of all blockchain nodes.

[0079] Specifically, the data carrying capacity information corresponding to all blockchain nodes is updated in real time and uploaded to the electronic equipment in real time. The data carrying capacity information corresponding to each blockchain

node can be the same or different.

[0080] Step C2: determining a target blockchain node that is not less than an expected carrying capacity information from all blockchain nodes based on the corresponding data carrying capacity information and expected carrying capacity information of all blockchain nodes, and the expected carrying capacity information is determined based on the monitoring information and the encrypted associated information.

[0081] Step C3: uploading the monitoring information and the encrypted associated information to the target blockchain node.

[0082] Specifically, the data carrying capacity information can refer to the current actual carrying capacity information of each blockchain node. The corresponding data carrying capacity information of all blockchain nodes is compared with the expected carrying capacity information one by one to determine whether it is not less than the expected carrying capacity information of the target blockchain node. In this context, the expected carrying capacity information can be calculated using the byte calculation method. The embodiment of the present disclosure does not limit the specific calculation process of the byte calculation method. Furthermore, after determining the target blockchain nodes, they can be arranged in descending order of data carrying capacity, and the blockchain nodes with the highest data carrying capacity can be selected as the target blockchain nodes, or the blockchain nodes with the same data carrying capacity and the expected carrying capacity information can be selected as the target blockchain nodes.

[0083] Based on the above embodiment, data carrying capacity information corresponding to each blockchain node is obtained, and the target blockchain node that is not less than the carrying information is determined from all blockchain nodes based on the data carrying capacity information and the expected carrying capacity information for each blockchain node. This is done to store monitoring information and encrypted associated information into the target blockchain node with a larger storage space, while also avoiding overloading or under-utilization of certain blockchain nodes, thus achieving efficient utilization of blockchain nodes.

[0084] Furthermore, in the embodiment of the present disclosure, after uploading the monitoring information and the encrypted associated information to the blockchain node, also including:

obtaining a reward corresponding to the expected carrying capacity information

based on the expected carrying capacity information, and sending the reward to the target blockchain node, wherein the target blockchain node is the blockchain node that uploads the monitoring information and the encrypted associated information.

[0085] Specifically, rewards can be obtained in real time, or alternatively, rewards can be obtained on a scheduled basis.

[0086] In a practical implementation, obtaining rewards in real time specifically includes: each time the monitoring information and the encrypted associated information are transmitted, the corresponding rewards can be obtained from the blockchain network;

[0087] In another practical implementation, obtaining rewards on a scheduled basis specifically includes: the electronic equipment periodically performs statistics on the monitoring information and the encrypted associated information, generates statistical values, and acquires corresponding rewards based on those statistical values.

[0088] Furthermore, sending rewards to the target blockchain node can enhance the participation enthusiasm of blockchain nodes through a reward mechanism.

[0089] Based on the above embodiment, corresponding rewards are obtained based on the expected carrying capacity information, so as to enhance the participation enthusiasm of each blockchain node in the blockchain network and ensure that participants of different dimensions can participate in the processing of data information.

[0090] Furthermore, in the embodiment of the present disclosure, Step 103 before establishing an associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers, also including:

obtaining an information format corresponding to the monitoring information, and judging whether the information format is a preset standard format.

[0091] Specifically, the information format of the monitoring information can be obtained by calling a function that utilizes a suffix name, such as the `strchr()` function, `explode()` function, or `pathinfo()` function. The embodiment of the present disclosure does not limit the specific content of the suffix name calling function, as long as it is capable of achieving the purpose of calling the suffix name as described in the present disclosure. In the embodiment of the present disclosure, for the convenience of storage, the preferred preset standard format can be JavaScript Object Notation (JSON) or Extensible Markup Language (XML).

[0092] If not, converting the information format corresponding to the monitoring

information into the preset standard format to obtain a format-converted monitoring information;

correspondingly, establishing the associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers, comprising:

establishing an associated information between the format-converted monitoring information, the first identity identifier, and the plurality of second identity identifiers.

[0093] Specifically, if the information format of the monitoring information is determined to not be the preset standard format, it can be converted to the preset standard format through an expression editor. The embodiment of the present disclosure does not limit the format conversion process of the expression editor, and users can set it up according to their own needs. Furthermore, establishing an associated information between the format-converted monitoring information, the first identity identifier, and the plurality of second identity identifiers to facilitate data storage.

[0094] Based on the above embodiment, obtaining an information format corresponding to the monitoring information, and judging whether the information format is a preset standard format. If not, it is converted into the preset standard format, and the format-converted monitoring information, the first identity identifier, and the second identity identifier are associated and the associated information is stored in a standard format, which can effectively improve data storage efficiency.

[0095] The above embodiments introduce a blockchain-based monitoring data processing method from the perspective of method flow. The following embodiments introduce a blockchain-based monitoring data processing device from the perspective of virtual modules or virtual units. Please see the details in the following embodiment.

[0096] An embodiment of the present disclosure provides a blockchain-based monitoring data processing device, as shown in FIG. 3. The blockchain-based monitoring data processing device may specifically include:

an acquisition module 210, wherein the acquisition module 210 is used for obtaining a monitoring information and a first identity identifier corresponding to a monitoring equipment, wherein the monitoring information is information obtained based on the analysis of monitoring images collected by the monitoring equipment, wherein the monitoring information comprises monitoring images and corresponding analysis results, and the monitoring image is either an image of a person or an image

of environmental changes;

a second identity identifier determination module 220, wherein the second identity identifier determination module 220 is used for determining a plurality of second identity identifiers corresponding to the first identity identifier based on the first identity identifier, wherein the second identity identifier is an identity identifier of a terminal equipment with access permission corresponding to the first identity identifier;

an associated information establishing module 230, wherein the associated information establishing module 230 is used for establishing an associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers; and

a storage module 240, wherein the storage module 240 is used for encrypting the associated information to obtain an encrypted associated information; and uploading the monitoring information and the encrypted associated information to a blockchain node.

[0097] A possible implementation in the embodiment of the present disclosure, the second identity identifier determination module 220, when executing the task of determining a plurality of second identity identifiers corresponding to the first identity identifier based on the first identity identifier, is used for:

obtaining a network information corresponding to the first identity identifier;

determining a plurality of to-be-determined equipment using the same network corresponding to the first identity identifier based on the network information;

obtaining an access history information corresponding to each of the plurality of to-be-determined equipment;

performing information category identification on the text information to determine the information category of the monitoring information;

selecting a plurality of target equipment from the plurality of to-be-determined equipment, whose accessing information categories match the categories of the information, wherein the accessing information categories are obtained through identifying the access history information; and

obtaining an equipment identifier corresponding to each of the plurality of target equipment, and determining the equipment identifier corresponding to each of the plurality of target equipment as the plurality of second identity identifiers corresponding to the first identity identifier.

[0098] A possible implementation in the embodiment of the present disclosure, encrypting the associated information to obtain an encrypted associated information, the storage module 240 is used for:

- obtaining a location information of the monitoring equipment, and determining a privacy level corresponding to an installation location information for the monitoring equipment based on a preset corresponding relationship between the location information and the privacy level and the installation location information for the monitoring equipment;

- determining a target information encryption policy based on the privacy level and a preset information encryption policy; and

- encrypting the associated information using the target information encryption policy to obtain the encrypted associated information.

[0099] A possible implementation in the embodiment of the present disclosure, a blockchain-based monitoring data processing device also includes:

- a monitoring information acquisition module is used for:

- obtaining multiple consecutive monitoring images within a preset duration;

- determining whether there is an image change based on the multiple consecutive monitoring images;

- if so, performing image recognition on a changed image to determine a category of the changed image, and the category of the changed image comprises: a personnel change, and/or an environmental change;

- if the category of the changed image is the personnel change, determining a personnel identification information based on the changed image, and the personnel identification information at least includes a personnel identity identifier and a personnel action event;

- if the category of the changed image is the environmental change, obtaining an environmental change data, and determining an environmental safety risk assessment information based on the environmental change data; and

- determining the multiple consecutive monitoring images and an image change information as the monitoring information, and the image change information comprises: the personnel identification information and/or the environmental safety risk assessment information.

[00100] A possible implementation in the embodiment of the present disclosure, when uploading the monitoring information and the encrypted associated information

to a blockchain node, the storage module 240 is used for:

- obtaining a data carrying capacity information corresponding to each of all blockchain nodes;

- determining a target blockchain node that is not less than an expected carrying capacity information from all blockchain nodes based on the corresponding data carrying capacity information and expected carrying capacity information of all blockchain nodes, and the expected carrying capacity information is determined based on the monitoring information and the encrypted associated information; and

- uploading the monitoring information and the encrypted associated information to the target blockchain node.

[00101] A possible implementation in the embodiment of the present disclosure, a blockchain-based monitoring data processing device also includes:

- a reward module is used for:

- obtaining a reward corresponding to the expected carrying capacity information based on the expected carrying capacity information, and sending the reward to the target blockchain node, wherein the target blockchain node is the blockchain node that uploads the monitoring information and the encrypted associated information.

[00102] A possible implementation in the embodiment of the present disclosure, a blockchain-based monitoring data processing device also includes:

- an information format judgment module is used for:

- obtaining an information format corresponding to the monitoring information, and judging whether the information format is a preset standard format;

- if not, converting the information format corresponding to the monitoring information into the preset standard format to obtain a format-converted monitoring information;

- correspondingly, when establishing an associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers, the associated information establishing module 230 is used for:

- establishing an associated information between the format-converted monitoring information, the first identity identifier, and the plurality of second identity identifiers.

[00103] Those skilled in the art can clearly understand, for the convenience and conciseness of description, the specific working process of the aforementioned blockchain-based monitoring data processing device can refer to the corresponding process in the aforementioned method embodiment, and thus will not be repeated

here.

[00104] An embodiment of the present disclosure provides an electronic equipment, as shown in FIG. 4, which is a structure schematic diagram of an electronic equipment provided by an embodiment of the present disclosure. The electronic equipment 300 shown in FIG. 4 includes: a processor 301 and a memory 303. The processor 301 and the memory 303 are connected, such as through a bus 302. Optionally, the electronic equipment 300 may also include a transceiver 304. It should be noted that in practical applications, the number of transceivers 304 is not limited to one, and the structure of the electronic equipment 300 does not constitute a limitation on the embodiments of the present disclosure.

[00105] The processor 301 may be a Central Processing Unit (CPU), a general-purpose processor, a Digital Signal Processor (DSP), Application Specific Integrated Circuit (ASIC), Field Programmable eGate Array (FPGA) or other programmable logic device, transistor logic device, hardware component, or any combination thereof. It may implement or execute various exemplary logical blocks, modules and circuits described in conjunction with the disclosure of the embodiments of the present disclosure. The processor 301 may also be a combination that implements computing functions, such as a combination of one or more microprocessors, a combination of a DSP and a microprocessor, etc.

[00106] The bus 302 may include a path that carries information between the above-mentioned components. The bus 302 may be a Peripheral Component Interconnect (PCI) bus or an Extended Industry Standard Architecture (EISA) bus, etc. The bus 302 can be divided into an address bus, a data bus, a control bus, etc. For ease of presentation, only one thick line is used in FIG. 4, but it does not mean that there is only one bus or one type of bus.

[00107] The memory 303 can be a Read Only Memory (ROM) or other types of static storage devices that can store static information and instructions, Random Access Memory (RAM) or other types of dynamic storage devices that can store information and instructions. It can also be Electrically Erasable Programmable Read Only Memory (EEPROM), Compact Disc Read Only Memory (CD-ROM) or other optical disc storage, including compressed discs, laser discs, disc, digital versatile discs, Blu-ray discs, etc., magnetic disk storage media or other magnetic storage devices, or any other medium that can be used to carry or store desired program codes in the form of instructions or data structures and can be accessed by a computer, but not limited to

these.

[00108] The memory 303 is used to store application program codes for executing solutions in the embodiments of the present disclosure, and is controlled by the processor 301 for execution. The processor 301 is used to execute the application program code stored in the memory 303 to implement the contents shown in the foregoing method embodiments.

[00109] The electronic equipment include but are not limited to: mobile terminals such as mobile phones, laptop computers, digital broadcast receivers, Personal Digital Assistant (PDA), Portable Android Device (PAD), Portable Multimedia Players (PMP), in-vehicle terminals (such as car navigation terminals), and so on, as well as fixed terminals such as digital Television (TV), desktop computers, and so on. The electronic equipment shown in FIG. 4 is only an example and should not impose any restrictions on the functions and usage scope of the embodiments of the present disclosure.

[00110] Embodiments of the present disclosure provides a computer-readable storage medium on which a computer program is stored. When the computer program runs on the computer, it enables the computer to execute the corresponding content of the aforementioned method embodiments.

[00111] It should be understood that although various steps in the flow chart of the accompanying drawings are shown in sequence as indicated by arrows, these steps are not necessarily executed in the order indicated by arrows. Unless explicitly stated in the present disclosure, the execution of these steps is not strictly limited in order, and they can be executed in other orders. Moreover, at least some of the steps in the flow chart of the accompanying drawings may include multiple sub-steps or multiple stages. These sub-steps or stages are not necessarily executed at the same time, but may be executed at different times, and the execution order is not necessarily sequential, but may be rotated or alternated with other steps or sub-steps of other steps or at least part of the stages.

[00112] The above are only some of the embodiments of the present disclosure, and it should be noted that for those ordinary skilled in the art, a number of improvements and modifications can be made without departing from the principles of the present disclosure, and these improvements and modifications should also be regarded as the scope of protection of the present disclosure.

CLAIMS

What is claimed is:

1. A blockchain-based monitoring data processing method, comprising:

obtaining a monitoring information and a first identity identifier corresponding to a monitoring equipment, wherein the monitoring information is information obtained based on the analysis of monitoring images collected by the monitoring equipment, wherein the monitoring information comprises monitoring images and corresponding analysis results, and the monitoring image is either an image of a person or an image of environmental changes;

determining a plurality of second identity identifiers corresponding to the first identity identifier based on the first identity identifier, wherein the second identity identifier is an identity identifier of a terminal equipment with access permission corresponding to the first identity identifier;

establishing an associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers;

encrypting the associated information to obtain an encrypted associated information; and uploading the monitoring information and the encrypted associated information to a blockchain node,

the monitoring information at least comprises: a text information,

determining the plurality of second identity identifiers corresponding to the first identity identifier based on the first identity identifier, comprising:

obtaining a network information corresponding to the first identity identifier;

determining a plurality of to-be-determined equipment using the same network corresponding to the first identity identifier based on the network information;

obtaining an access history information corresponding to each of the plurality of to-be-determined equipment;

performing information category identification on the text information to determine the information category of the monitoring information;

selecting a plurality of target equipment from the plurality of to-be-determined equipment, whose accessing information categories match the categories of the information, wherein the accessing information categories are obtained through identifying the access history information; and

obtaining an equipment identifier corresponding to each of the plurality of target equipment, and determining the equipment identifier corresponding to each of the

plurality of target equipment as the plurality of second identity identifiers corresponding to the first identity identifier.

2. The blockchain-based monitoring data processing method according to claim 1, wherein encrypting the associated information to obtain the encrypted associated information comprises:

obtaining a location information of the monitoring equipment, and determining a privacy level corresponding to an installation location information for the monitoring equipment based on a preset corresponding relationship between the location information and the privacy level and the installation location information for the monitoring equipment;

determining a target information encryption policy based on the privacy level and a preset information encryption policy; and

encrypting the associated information using the target information encryption policy to obtain the encrypted associated information.

3. The blockchain-based monitoring data processing method according to claim 1, wherein obtaining the monitoring information comprises:

obtaining multiple consecutive monitoring images within a preset duration;

determining whether there is an image change based on the multiple consecutive monitoring images;

if so, performing image recognition on a changed image to determine a category of the changed image, and the category of the changed image comprises: a personnel change, and/or an environmental change;

if the category of the changed image is the personnel change, determining a personnel identification information based on the changed image, and the personnel identification information at least includes a personnel identity identifier and a personnel action event;

if the category of the changed image is the environmental change, obtaining an environmental change data, and determining an environmental safety risk assessment information based on the environmental change data; and

determining the multiple consecutive monitoring images and an image change information as the monitoring information, and the image change information comprises: the personnel identification information and/or the environmental safety risk assessment information.

4. The blockchain-based monitoring data processing method according to claim

1, wherein uploading the monitoring information and the encrypted associated information to the blockchain node comprises:

obtaining a data carrying capacity information corresponding to each of all blockchain nodes;

determining a target blockchain node that is not less than an expected carrying capacity information from all blockchain nodes based on the corresponding data carrying capacity information and expected carrying capacity information of all blockchain nodes, and the expected carrying capacity information is determined based on the monitoring information and the encrypted associated information; and

uploading the monitoring information and the encrypted associated information to the target blockchain node.

5. The blockchain-based monitoring data processing method according to claim 4, wherein after uploading the monitoring information and the encrypted associated information to the blockchain node, further comprising:

obtaining a reward corresponding to the expected carrying capacity information based on the expected carrying capacity information, and sending the reward to the target blockchain node, wherein the target blockchain node is the blockchain node that uploads the monitoring information and the encrypted associated information.

6. The blockchain-based monitoring data processing method according to claim 1, wherein before establishing the associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers, further comprising:

obtaining an information format corresponding to the monitoring information, and judging whether the information format is a preset standard format;

if not, converting the information format corresponding to the monitoring information into the preset standard format to obtain a format-converted monitoring information;

correspondingly, establishing the associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers, comprising:

establishing an associated information between the format-converted monitoring information, the first identity identifier, and the plurality of second identity identifiers.

7. A blockchain-based monitoring data processing device, comprising:

an acquisition module, wherein the acquisition module is used for obtaining a

monitoring information and a first identity identifier corresponding to a monitoring equipment, wherein the monitoring information is information obtained based on the analysis of monitoring images collected by the monitoring equipment, wherein the monitoring information comprises monitoring images and corresponding analysis results, and the monitoring image is either an image of a person or an image of environmental changes;

a second identity identifier determination module, wherein the second identity identifier determination module is used for determining a plurality of second identity identifiers corresponding to the first identity identifier based on the first identity identifier, wherein the second identity identifier is an identity identifier of a terminal equipment with access permission corresponding to the first identity identifier;

an associated information establishing module, wherein the associated information establishing module is used for establishing an associated information between the monitoring information, the first identity identifier, and the plurality of second identity identifiers; and

a storage module, wherein the storage module is used for encrypting the associated information to obtain an encrypted associated information; and uploading the monitoring information and the encrypted associated information to a blockchain node,

the monitoring information at least comprises: a text information,

a second identity identifier determination module, wherein the second identity identifier determination module is used for:

obtaining a network information corresponding to the first identity identifier;

determining a plurality of to-be-determined equipment using the same network corresponding to the first identity identifier based on the network information;

obtaining an access history information corresponding to each of the plurality of to-be-determined equipment;

performing information category identification on the text information to determine the information category of the monitoring information;

selecting a plurality of target equipment from the plurality of to-be-determined equipment, whose accessing information categories match the categories of the information, wherein the accessing information categories are obtained through identifying the access history information; and

obtaining an equipment identifier corresponding to each of the plurality of target

equipment, and determining the equipment identifier corresponding to each of the plurality of target equipment to be the plurality of second identity identifiers corresponding to the first identity identifier.

8. An electronic equipment, comprising:

at least one processor;

a memory; and

at least one application program, wherein at least one application program is stored in the memory and configured to be executed by at least one processor, the at least one application program is configured to: execute the blockchain-based monitoring data processing method according to any one of claims 1 to 6.

9. A computer-readable storage medium, wherein a computer program is stored thereon, and when the computer program is executed in a computer, the computer is executed the blockchain-based monitoring data processing method according to any one of claims 1 to 6.