

METHOD, APPARATUS, AND ELECTRONIC DEVICE FOR BLOCKCHAIN-BASED RECORDKEEPING

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to the Chinese patent application No. 201811289523.7 filed on October 31, 2018, and entitled "METHOD, APPARATUS, AND ELECTRONIC DEVICE FOR BLOCKCHAIN-BASED RECORDKEEPING," which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] One or more embodiments of the application relate to the field of blockchain technologies, and in particular, to a method, apparatus, and electronic device for blockchain-based recordkeeping.

BACKGROUND

[0003] Blockchain, also known as a distributed ledger technology, is an emerging technology in which multiple computing devices participate in "accounting" to maintain a complete distributed database jointly. The blockchain technology is decentralized and transparent, each computing device can participate in maintaining records in the database, and data can be quickly synchronized among the computing devices. With the aforementioned characteristics, the blockchain technology has been widely applied in many fields.

SUMMARY

[0004] This specification provides a method for blockchain-based data verification, and the method may include: obtaining target data submitted by a data submitter, wherein a first data digest of the target data is recorded in a blockchain; computing a second data digest of the target data; determining whether the second data digest matches the first data digest of the target data recorded in the blockchain; and determining that the target data submitted by the data submitter is valid in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain.

[0005] In some embodiments, the method may further comprise: determining that the target data submitted by the data submitter is invalid in response to determining that the second data digest does not match the first data digest of the target data recorded in the blockchain.

[0006] In some embodiments, the target data is acquired by a terminal device, the terminal

device comprises a secure operation environment, and a private key of the terminal device is stored in the secure operation environment.

[0007] In some embodiments, the method may further comprise: obtaining the first data digest of the target data submitted by the terminal device to the blockchain, wherein the first data digest is signed in the secure operation environment based on the private key of the terminal device to generate a signature; the signature of the first data digest is verified based on a public key corresponding to the private key; and the first data digest of the target data is recorded in the blockchain in response to the signature being verified to be valid.

[0008] In some embodiments, the terminal device comprises a body worn camera or an event data recorder. In some embodiments, the target data comprises video data, audio data, or image data, or a combination thereof, which is acquired by the body worn camera or the event data recorder.

[0009] In some embodiments, determining whether the second data digest matches the first data digest of the target data recorded in the blockchain comprises: verifying whether the second data digest has been recorded in the blockchain; and determining that the second data digest matches the first data digest of the target data recorded in the blockchain in response to verifying that the second data digest has been recorded in the blockchain.

[0010] In some embodiments, determining whether the second data digest matches the first data digest of the target data recorded in the blockchain further comprises: determining that the second data digest does not match the first data digest of the target data recorded in the blockchain in response to verifying that the second data digest has not been recorded in the blockchain.

[0011] In some embodiments, determining whether the second data digest matches the first data digest of the target data recorded in the blockchain comprises: obtaining the first data digest of the target data recorded in the blockchain; determining whether the first data digest of the target data is the same as the second data digest; and determining that the second data digest matches the first data digest of the target data recorded in the blockchain in response to determining that the first data digest of the target data is the same as the second data digest.

[0012] In some embodiments, determining whether the second data digest matches the first data digest of the target data recorded in the blockchain further comprises: determining that the second data digest does not match the first data digest of the target data recorded in the blockchain in response to determining that the first data digest of the target data is different

from the second data digest.

[0013] In some embodiments, description data of the target data is recorded in the blockchain; and determining that the target data submitted by the data submitter is valid in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain comprises: in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain, determining whether description data of the target data submitted by the data submitter matches the description data of the target data recorded in the blockchain; and determining that the target data submitted by the data submitter is valid in response to determining that the description data of the target data submitted by the data submitter matches the description data of the target data recorded in the blockchain.

[0014] In some embodiments, the description data comprises: an acquisition time of the target data, an acquisition location of the target data, or an object related to the target data, or a combination thereof.

[0015] This specification further provides an apparatus for blockchain-based data verification, and the apparatus may include: one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the apparatus to perform operations comprising: obtaining target data submitted by a data submitter, wherein a first data digest of the target data is recorded in a blockchain; computing a second data digest of the target data; determining whether the second data digest matches the first data digest of the target data recorded in the blockchain; and determining that the target data submitted by the data submitter is valid in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain.

[0016] This specification further provides a non-transitory computer-readable storage medium. The non-transitory computer-readable storage medium may be configured with instructions executable by one or more processors to cause the one or more processors to perform operations comprising: one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the apparatus to perform operations comprising: obtaining target data submitted by a data submitter, wherein a first data digest of the target data is recorded in a blockchain; computing a second data digest of

the target data; determining whether the second data digest matches the first data digest of the target data recorded in the blockchain; and determining that the target data submitted by the data submitter is valid in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain.

[0017] In the foregoing technical solutions, in one aspect, by improving the process of recordkeeping on the blockchain, the terminal device may no longer needs to record original content of acquired data on the blockchain; instead, the terminal device locally stores the original content of the acquired data, and records a data digest of the original content on the blockchain, so that the terminal device can be used as a hub between a physical world and a world on chain, and the acquired data is recorded on the blockchain more conveniently.

[0018] In another aspect, for a data verification party that obtains data acquired by the terminal device, the data verification party can conveniently verify the validity of the obtained data by matching a data digest of the obtained data with the data digest of the data which is recorded on the blockchain. Therefore, the data acquired by the terminal device can be submitted to the data verification party as proof or evidence, thereby greatly improving the usability of the data acquired by the terminal device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] FIG. 1 is a flowchart of a method for blockchain-based recordkeeping according to some embodiments;

[0020] FIG. 2 is a schematic structural diagram of an electronic device for blockchain-based recordkeeping according to some embodiments; and

[0021] FIG. 3 is a block diagram of an apparatus for blockchain-based recordkeeping according to some embodiments.

DETAILED DESCRIPTION

[0022] Because data stored on a blockchain cannot be tampered with, storing data on a blockchain for recordkeeping is a dominant trend in the industry at present.

[0023] However, in actual applications, some stream data, such as video stream and audio stream acquired by a body-worn camera or an event data recorder, may occupy a relatively large storage space, and therefore usually cannot be directly stored on the blockchain for recordkeeping.

[0024] However, in some scenarios, there is a strong demand to record such stream data. For example, in a judicial recordkeeping scenario, video stream acquired by a body-worn

camera or an event data recorder may be submitted as proof or evidence to a judicial department.

[0025] Due to the lack of data authentication means, usually, the validity of such stream data as proof or evidence is widely questioned. Therefore, the best processing manner for such stream data is to store the data on the blockchain for recordkeeping. Moreover, storing data on blockchain for recordkeeping also makes it more convenient to verify the validity of the recorded data as judicial proof or evidence.

[0026] This specification provides embodiments in which a terminal device is used as a hub between a physical world and a world on the blockchain, so that data acquired by the terminal device is recorded on a blockchain more conveniently; and the validity of the recorded data is verified quickly.

[0027] During implementation, after acquiring data to be recorded on a blockchain, the terminal device may store the acquired data locally, compute a data digest of the acquired data, and then submit the computed data digest of the data to the blockchain for recordkeeping in the blockchain.

[0028] For example, a hardware environment of the terminal device may be improved. A secure operation environment is set up in the hardware environment of the terminal device, and a private key corresponding to the terminal device is stored and maintained in the secure operation environment. After computing a data digest of acquired data, the terminal device may sign the computed data digest in the secure operation environment based on the private key of the terminal device to generate a signature, and then submit the signed data digest along with the signature to the blockchain. After receiving the signed data digest submitted by the terminal device, a node in the blockchain may obtain a public key corresponding to the private key of the terminal device, and then verify the signature of the data digest based on the public key; if the signature is verified to be valid, the data digest may be stored in the blockchain for recordkeeping.

[0029] After the terminal device completes recordkeeping of the acquired data on the blockchain, a data submitter/provider may submit original content of the data, which is locally stored on the terminal device, to a data verification party as proof or evidence.

[0030] After receiving the data submitted by the data provider, the data verification party computes a data digest of the data, and determines whether the computed data digest matches the data digest of the data which has been recorded in the blockchain for recordkeeping.

[0031] If the computed data digest matches the data digest of the data which has been recorded in the blockchain, the data verification party can determine that the data submitted by the data submitter is valid data; on the contrary, if the computed data digest does not match the data digest of the data which has been recorded in the blockchain, the data verification party can determine that the data submitted by the data submitter is invalid data.

[0032] In the foregoing embodiments, in one aspect, by improving the process of recordkeeping on the blockchain, the terminal device may no longer need to record original content of acquired data on the blockchain; instead, the terminal device may locally store the original content of the acquired data, and record a data digest of the original content on the blockchain, so that the terminal device can be used as a hub between a physical world and a world on the blockchain, and the acquired data is recorded on the blockchain more conveniently.

[0033] In another aspect, for a data verification party that obtains data acquired by the terminal device, the data verification party can conveniently verify the validity of the obtained data by matching a data digest of the obtained data with a data digest of the data which has been recorded on the blockchain. Therefore, the data acquired by the terminal device can be submitted to the data verification party as proof or evidence, thereby greatly improving the usability of the data acquired by the terminal device.

[0034] Referring to FIG. 1, FIG. 1 shows a method for blockchain-based recordkeeping according to some embodiments of this specification. The method is implementable by a data verification party, where a first data digest of target data acquired by a terminal device is recorded in the blockchain. The following steps are performed according to the method.

[0035] Step 102: Obtaining target data submitted by a data submitter.

[0036] Step 104: Computing a second data digest of the target data.

[0037] Step 106: Determining whether the computed second data digest matches the first data digest of the target data which has been recorded in the blockchain.

[0038] Step 108: Determining that the target data submitted by the data submitter is valid in response to determining that the computed second data digest matches the first data digest of the target data which has been recorded in the blockchain; and determining that the target data submitted by the data submitter is invalid in response to determining that the computed second data digest does not match the first data digest of the target data which has been recorded in the blockchain.

[0039] In some embodiments, the blockchain described may be a private blockchain, a public blockchain, a consortium blockchain, or the like. Alternatively, other types of blockchain may also be used.

[0040] For example, the blockchain may be a consortium blockchain having the following member devices: a server of a third-party payment platform, a domestic bank server, an offshore bank server, and multiple user nodes. An entity operating the consortium blockchain may deploy online services such as consortium-blockchain-based cross-border account transfer and asset transfer.

[0041] In some embodiments, the terminal device may be any form of terminal device that can be added to the blockchain network as a node and can submit acquired data to the blockchain for recordkeeping. For example, the terminal device may include a body-worn camera, an event data recorder, or the like. The body-worn camera or the event data recorder may be added to the blockchain network as a node and submit acquired stream data, such as video data and audio data, to the blockchain for recordkeeping.

[0042] Recording data on the blockchain for recordkeeping may include permanently storing the data as proof or evidence on the blockchain.

[0043] In some embodiments, the target data may be any type of data that can be acquired by the terminal device and can be recorded in a distributed database of the blockchain network. For example, the target data may be stream data, such as video data, audio data, and image stream data, acquired by a terminal device such as a body-worn camera or an event data recorder.

[0044] In some embodiments, a hardware environment of the terminal device may be improved. A secure operation environment is set up in the hardware environment of the terminal device, and a private key corresponding to the terminal device is stored and maintained in the secure operation environment. The secure operation environment is provided for the terminal device.

[0045] Different manners may be used to set up the secure operation environment in the hardware environment of the terminal device.

[0046] For example, the secure operation environment may be set up by introducing new hardware to the hardware environment of the terminal device, or the secure operation environment may be set up by improving a software environment of existing hardware in the hardware environment of the terminal device. Alternatively, the secure operation

environment may be set up by both introducing new hardware to the hardware environment of the terminal device and improving a software environment of existing hardware in the hardware environment of the terminal device.

[0047] For example, a secure operation environment may be set up for the terminal device based on a secure element (SE). For example, SE hardware may be introduced to the hardware environment of the terminal device. The SE hardware may be built-in hardware in the hardware environment of the terminal device, or may be external hardware connected to the terminal device through an interface. The private key corresponding to the terminal device is stored and maintained by using the SE hardware, and the secure operation environment is provided for the terminal device.

[0048] In another example, a secure operation environment may be set up for the terminal device based on a Trusted Execution Environment (TEE). For example, a software environment of existing hardware (such as a main chip) in the hardware environment of the terminal device may be improved to set up a trusted execution environment in the software environment. The private key corresponding to the terminal device is stored and maintained in the trusted execution environment, and the secure operation environment is provided for the terminal device.

[0049] In a third example, a secure operation environment may be set up for the terminal device based on both SE and TEE. For example, the private key corresponding to the terminal device may be stored and maintained by using SE hardware, and the secure operation environment is provided for the terminal device by using a TEE.

[0050] The foregoing embodiments of setting up the secure operation environment for the terminal device are merely examples. In actual applications, the secure operation environment may also be set up for the terminal device by using other implementation means, and the implementation means are not enumerated.

[0051] In some embodiments, the terminal device may be added to the blockchain network as a node (which is also referred to as placing a device onto the blockchain), and the private key corresponding to the terminal device is stored and maintained in the secure operation environment set up for the terminal device.

[0052] The private key corresponding to the terminal device may be a private key owned by the terminal device, or may be a private key owned by a user of the terminal device. For example, "the private key corresponding to the terminal device" described may be a private

key that is generated by a device manufacturer of the terminal device for the terminal device during a device manufacturing stage and is owned by the terminal device; or may be a private key that is generated autonomously by the terminal device for a user when the user uses the terminal device and is owned by the user.

[0053] In some embodiments, the private key and the public key owned by the terminal device may be generated by the device manufacturer for the terminal device during the device manufacturing stage, and the device manufacturer may write the private key into the secure operation environment of the terminal device in advance for storage and maintenance. Thus, the private key and the public key owned by the terminal device may not be associated with the identity of a user of the terminal device. Different users of the terminal device can share the same private key written into the secure operation environment of the terminal device by the device manufacturer by default.

[0054] In other embodiments, the private key and the public key owned by the terminal device may be generated autonomously by the terminal device for a user of the terminal device, and the terminal device autonomously writes the private key into the secure operation environment of the terminal device. Thus, the private key and the public key autonomously generated by the terminal device may be associated with the identity of a user of the terminal device. Based on identity information of different users, the terminal device may generate a pair of private key and public key for each user, associate the generated private keys with the identity information of the users, and then store and maintain the private keys, the identity information of the users, and association relationships of the private keys and the identity information of the users in the secure operation environment.

[0055] For example, during implementation, the manufacturer of the terminal device may write a key generating algorithm into the secure operation environment of the terminal device in advance. When a user of the terminal device uses the terminal device, the terminal device may prompt the user to input identity information for identity authentication. A data type of the identity information input by the user and an identity authentication manner used by the terminal device are not limited. For example, a conventional authentication manner of inputting a password or a token may be used, or an authentication manner based on a physiological feature such as a fingerprint or a human face may be used.

[0056] After the terminal device obtains the identity information input by the user, it can be determined whether a private key associated with the identity information is stored in the

secure operation environment. If the private key associated with the identity information is not stored in the secure operation environment, it may indicate that the user is a new user using the terminal device for the first time. In this situation, the terminal device can perform identity authentication on the user based on the obtained identity information. If the identity authentication on the user succeeds, the terminal device may invoke the key generating algorithm in the secure operation environment to generate a pair of private key and public key, associate the generated private key with the identity information of the user, and then store and maintain the private key, the identity of the user, and an association relationship between the private key and the identity of the user in the secure operation environment.

[0057] In some embodiments, the user may acquire data by using the terminal device, and record the acquired data on the blockchain by using the terminal device.

[0058] In some embodiments, the terminal device may store acquired data locally, and record, on the blockchain, a data digest of the acquired data. The terminal device may no longer record original content of the acquired data on the blockchain.

[0059] In some embodiments, if the target data acquired by the terminal device is stream data such as video stream data and audio stream data, when recording such stream data on the blockchain, the terminal device may record the stream data in a fragmented manner according to a preset time cycle.

[0060] For example, taking video data as an example, the terminal device may use video data in every N minute as a fragment (e.g., N is an integer), compute a data digest of the fragment, then record the data digest of the fragment on the blockchain. In addition, the terminal device may strictly ensure a chronological order of data digests of fragments recorded on the blockchain to facilitate tracing of the data digests and fragments.

[0061] In some embodiments, when recording the acquired target data on the blockchain, the terminal device may first compute a data digest of the target data. For example, the data digest may be a hash value of the target data computed based on a hash algorithm. Then, the terminal device may sign the data digest in the secure operation environment based on the private key stored in the secure operation environment.

[0062] In some embodiments, device authentication information signed based on a private key owned by a manufacturer of the terminal device may further be stored and maintained in the secure operation environment of the terminal device. For example, the manufacturer of the terminal device may sign the device authentication information based on a private key of

the manufacturer during a device manufacturing stage (e.g., to generate a signature of the device authentication information), and then write the signed device authentication information into the secure operation environment for storage and maintenance. The device authentication information may be any form of information that can be used for authenticating the validity of the terminal device. For example, the device authentication information may be a production number of the terminal device, or anti-counterfeit information in other forms.

[0063] Before signing the data digest in the secure operation environment based on the private key stored in the secure operation environment, the terminal device may obtain a public key corresponding to the private key owned by the manufacturer of the terminal device, and verify the signature of the device authentication information based on the obtained public key. If the verification succeeds, it can be determined that the terminal device is a valid terminal device manufactured by the manufacturer. Thus, the terminal device further signs the data digest in the secure operation environment based on the private key stored in the secure operation environment.

[0064] In this way, validity verification of the terminal device may be introduced before the digest data on the blockchain is signed based on the private key stored in the secure operation environment, to prevent behaviors of storing data onto the blockchain by some invalid devices (for example, a forged device or a maliciously modified invalid device) in time, thereby improving the security level of data to be recorded on the blockchain.

[0065] In some embodiments, if the private key stored and maintained in the secure operation environment of the terminal device is a private key that is generated by the device manufacturer for the terminal device in the device manufacturing stage and owned by the terminal device, then an identity authentication mechanism for a user of the terminal device may be initiated to prompt the user to input the user's identity information for identity authentication of the user. After obtaining the identity information input by the user, the terminal device may perform identity authentication on the user based on the obtained identity information. If the identity authentication on the user succeeds (i.e., the identity information of the user is valid), the terminal device may sign the data digest in the secure operation environment based on the private key stored and maintained in the secure operation environment and owned by the terminal device.

[0066] In some embodiments, if the private key of the terminal device stored and

maintained in the secure operation environment is a private key that is autonomously generated by the terminal device for a user and owned by the user, then an association relationship between the identity information and the private key of the user is stored and maintained in the secure operation environment in advance.

[0067] In this situation, after obtaining identity information input by the user, the terminal device may query the association relationship maintained in the secure operation environment to determine whether a private key associated with the identity information is stored in the secure operation environment. If the private key associated with the identity information is stored in the secure operation environment, the terminal device may sign the data digest in the secure operation environment based on the private key.

[0068] If the private key associated with the identity information is not stored in the secure operation environment, it may indicate that the user is a new user using the terminal device for the first time. In this situation, the terminal device can perform identity authentication on the user based on identity information of the user. After the identity authentication succeeds, the terminal device invokes a key generating algorithm stored in the secure operation environment to generate a private key and a public key for the user, signs the data digest by using the generated private key, associates the generated private key with the identity information of the user, and then stores and maintains an association relationship between the generated private key and the identity information of the user in the secure operation environment.

[0069] In some embodiments, after signing the data digest of the acquired target data in the secure operation environment based on the private key stored in the secure operation environment, the terminal device may submit the signed data digest in the blockchain.

[0070] For example, a blockchain-based transaction may be constructed based on the signed data digest, and the transaction is broadcast and spread to other nodes.

[0071] After receiving the signed data digest, a node in the blockchain may obtain a public key corresponding to the private key stored in the secure operation environment, and then verify the signature based on the obtained public key. If the signature is verified to be valid, the node can initiate, in the blockchain, consensus processing for the data digest. After the data digest passes the consensus processing, the node packages the data digest into a block to be stored in the blockchain, so as to complete recordkeeping for the data digest.

[0072] Different consensus mechanisms may be used by the blockchain. For example, an

entity operating the blockchain may select a consensus mechanism flexibly based on an actual requirement.

[0073] In some embodiments, when recording the acquired target data on the blockchain, the terminal device may further record description data of the target data along with the data digest of the target data on the blockchain.

[0074] For example, when signing the data digest of the target data in the secure operation environment based on the private key stored in the secure operation environment, the terminal device may sign the data digest and the description information of the target data as a whole. That is, the data digest and the description information of the target data are packaged and then signed as a whole, and the signed data digest and description data of the target data are submitted to the blockchain for recordkeeping.

[0075] For example, the terminal device may construct a blockchain-based transaction based on the signed data digest and description data of the target data, and broadcast and spread the transaction to other nodes.

[0076] Alternatively, when signing the data digest of the target data in the secure operation environment based on the private key stored in the secure operation environment, the terminal device may sign the data digest only, and then submit the description data of the target data and the signed data digest to the blockchain for recordkeeping.

[0077] For example, the terminal device may construct a blockchain-based transaction based on the description data of the target data and the signed data digest, and broadcast and spread the transaction to other nodes.

[0078] The description information of the target data may include any content. For example, the description information may contain any content related to the target data in actual applications.

[0079] In some embodiments, the acquisition time of the data, the acquisition location of the data, and the object related to the acquired data are usually crucial attributes of the data as evidence or proof. Therefore, in some embodiments, the description information of the target data may include one of the acquisition time of the data, the acquisition location of the data, and the object related to the acquired data, or a combination thereof.

[0080] In some embodiments, the acquisition time of target data may be a certified authoritative moment (timestamp) obtained from a time certificate authority by interacting

with the time certificate authority when the terminal device obtains the target data. The acquisition location of the target data may be a precise acquisition site obtained by invoking, in real time, a positioning module (such as a Global Positioning System (GPS) module) included in the terminal device when the terminal device acquires the target data. The object related to the target data may be a related object manually input by a valid user of the terminal device after the terminal device acquires the target data.

[0081] Taking forensic video data of a car accident acquired by a body-worn camera as an example, description information of the video data may include a certified authoritative moment (i.e., acquisition time) obtained from the time certificate authority at the moment when the video data is acquired, a precise acquisition location obtained by the body-worn camera through invoking the positioning module in real time at the moment when the video data is acquired, and vehicle information, driver information, and the like, related to the video data, which are input by a law enforcer.

[0082] In some embodiments, after the terminal device finishes recording the data digest of the acquired target data on the blockchain, the node in the blockchain may return, to the terminal device, a notification message (for example, a recordkeeping receipt) indicating that the data digest of the target data has been recorded on the blockchain.

[0083] The notification message may include description information related to recordkeeping of the data digest of the target data on the blockchain. For example, the notification message may include a transaction ID of the transaction in which the data digest of the target data is used, the number of a block where the data digest of the target data is located, and the like.

[0084] Subsequently, the data submitter may submit the original content of the target data stored locally on the terminal device to a data verification party as proof or evidence.

[0085] The data submitter may be a user of the terminal device (for example, a data collector), or may be a third-party user having the authority to use the data locally stored in the terminal device. Alternatively, the data submitter may be other individual or entities submitting the data as proof or evidence.. The data verification party may be an individual, entity, or authority department using and verifying the data as the proof or evidence.

[0086] For example, if the terminal device is an event data recorder, when a vehicle of a user has a car accident and the user is to file a claim with an insurance company, the user may submit video data acquired by the event data recorder during driving of the vehicle to the

insurance company as an evidence document. The insurance company may verify the validity of the evidence document, and decide, based on a validity verification result of the evidence document, whether to settle the claim of the user.

[0087] In another example, if the terminal device is a body worn camera, when a law enforcer collects proof or evidence in cooperation with a judicial institution, video data of a law enforcement process acquired by the body worn camera during the law enforcement process may be submitted to the judicial institution as an evidence document. The judicial institution may verify the validity of the evidence document, and decide, based on a validity verification result of the evidence document, whether the evidence document can be used for judicial purposes.

[0088] In some embodiments, after the data verification party obtains the target data submitted by the data provider/submitter, because the terminal device has recorded the data digest of the target data on the blockchain, the data verification party can re-compute a data digest of the target data submitted by the data provider, and determine whether the re-computed data digest matches the data digest of the target data recorded on the blockchain, so as to verify the validity of the target data submitted by the data submitter.

[0089] In some embodiments, when determining whether the re-computed data digest matches the data digest of the target data which has been recorded on the blockchain, the data verification party may first obtain a data digest of the target data which has been recorded on the blockchain.

[0090] For example, the data submitter may submit, to the data verification party, the transaction ID of the transaction in which the data digest of the target data is used and the number of the block where the data digest of the target data is located (for example, information include in the recordkeeping receipt). The data verification party may search for the data digest of the target data in the blocks of the blockchain by using the transaction ID of the transaction in which the data digest of the target data is used and the block number as query indexes.

[0091] After obtaining the data digest of the target data which has been recorded on the blockchain, the data verification party may compare the re-computed data digest with the data digest of the target data which has been recorded on the blockchain to determine whether the two data digests are the same. If the two data digests are the same, it can be determined that the re-computed data digest matches the data digest of the target data which has been

recorded on the blockchain; and if the two data digests are different, it can be determined that the re-computed data digest does not match the data digest of the target data which has been recorded on the blockchain.

[0092] In other embodiments, the data verification party may determine whether the re-computed data digest matches the data digest of the target data which has been recorded on the blockchain, without obtaining the data digest of the target data which has been recorded on the blockchain.

[0093] For example, the data verification party may apply a verification algorithm. The verification algorithm is used for verifying whether a computed data digest has been recorded on the blockchain. The data verification party may execute the verification algorithm, and based on an execution result of the verification algorithm (where, for example, the execution result is usually true or false), verify whether the computed data digest has been recorded on the blockchain.

[0094] If the execution result of the verification algorithm indicates that the computed data digest has been recorded on the blockchain, then it can be determined that the computed data digest matches the data digest of the target data which has been recorded on the blockchain; if the execution result of the verification algorithm indicates that the computed data digest has not been recorded on the blockchain, it can be determined that the computed data digest does not match the data digest of the target data which has been recorded on the blockchain.

[0095] In some embodiments, when the data verification party determines, through verification, that the computed data digest does not match the data digest of the target data which has been recorded on the blockchain, it can be determined that the target data submitted by the data submitter is invalid data. On the contrary, when the data verification party determines, through verification, that the computed data digest matches the data digest of the target data which has been recorded on the blockchain, it can be determined that the target data submitted by the data submitter is valid data.

[0096] In some embodiments, in the recordkeeping stage, if the terminal device records the description data of the target data along with the data digest of the target data on the blockchain, the data submitter may also submit the description data of the target data to the data verification party along with the data digest of the target data.

[0097] Thus, when determining, through the foregoing validity verification processes, that the data digest of the target data submitted by the data submitter matches the data digest of

the target data which has been recorded on the blockchain, the data verification party may further determine whether the description data of the target data submitted by the data provider matches the description data of the target data which has been recorded on the blockchain.

[0098] For example, the data verification party may separately verify whether an acquisition time of the target data, an acquisition location of the target data, and an object related to the target data that are submitted by the data submitter match an acquisition time of the target data, an acquisition location of the target data, and an object related to the target data that are recorded on the blockchain.

[0099] If the verification succeeds, it is determined that the description data of the target data submitted by the data provider matches the description data of the target data which has been recorded on the blockchain, and then it is determined that the target data submitted by the data submitter is valid data. On the contrary, if it is determined, through the verification, that the description data of the target data submitted by the data provider does not match the description data of the target data which has been recorded on the blockchain, then it can be determined that the target data submitted by the data submitter is invalid data.

[00100] In this way, the verification of whether the description data of the target data submitted by the data provider matches the description data of the target data which has been recorded on the blockchain can be further introduced into the validation verification process described in the foregoing embodiments. It is determined that the target data submitted by the data submitter/provider is valid data when the data digest and the description data of the target data submitted by the data provider match the data digest and the description data of the target data which are recorded on the blockchain. Therefore, the error rate during validity verification can be reduced.

[00101] For example, if the target data is video data, the data provider may forge information of an acquisition time, or an acquisition location of the video data, or an object data related to the video data, and then submit the forged information along with the video data to the data verification party as proof or evidence. Therefore, by introducing the verification of whether the description data of the target data submitted by the data provider matches the description data of the target data recorded on the blockchain into the validation verification process described in the foregoing embodiments, such situations can be detected in time and prevented, thereby minimizing the probability of determining the video data as

valid data.

[00102] In one aspect, by improving the process of recordkeeping on the blockchain, the terminal device may no longer need to record original content of acquired data on the blockchain. Instead, the terminal device may locally store the original content of the acquired data, and records a data digest of the original content on the blockchain, so that the terminal device can be used as a hub between a physical world and a world on the blockchain, and the acquired data is recorded on the blockchain more conveniently.

[00103] In another aspect, for a data verification party that obtains data acquired by the terminal device, the data verification party can conveniently verify the validity of the obtained data by matching a data digest of the obtained data with a data digest of the data which has been recorded on the blockchain. Therefore, the data acquired by the terminal device can be submitted to the data verification party as proof or evidence, greatly improving the usability of the data acquired by the terminal device.

[00104] For example, when a user submits stream data acquired by a body worn camera or an event data recorder to a third-party institution (such as a judicial institution or an insurance company) as proof or evidence, the third-party institution may only need to re-compute a data digest of the obtained data and match the data digest of the data with the data digest of the data which has been recorded on the blockchain, thereby conveniently verifying the validity of the obtained data. In this way, usability of data acquired by the body worn camera or the event data recorder as valid proof or evidence can be significantly improved.

[00105] Similar to the foregoing method embodiments, this specification further provides some embodiments of an apparatus for blockchain-based recordkeeping. The embodiments of the apparatus for blockchain-based recordkeeping in this specification may be applied to an electronic device. The apparatus embodiments may be implemented by software, hardware, or a combination of software and hardware. Taking software implementation as an example, at a logical level, the apparatus is formed in the following manner: a processor of the electronic device where the apparatus is located reads corresponding computer program instructions in a non-volatile storage into an internal memory and executes the computer program instructions. At a hardware level, FIG. 2 is a structural diagram of hardware of an electronic device where the apparatus for blockchain-based recordkeeping according to this specification is located. In addition to a processor, an internal memory, a network interface, and a non-volatile storage shown in FIG. 2, the electronic device where the apparatus is

located usually may further include other hardware according to actual functions of the electronic device, and details are not described herein.

[00106] Referring to FIG. 3, FIG. 3 is a block diagram of an apparatus for blockchain-based recordkeeping according to some embodiments. The apparatus 30 for blockchain-based recordkeeping may be applied to the electronic device shown in FIG. 2. For example, the electronic device in FIG. 2 is a terminal device. The apparatus 30 may include: an obtaining module 301, a computing module 302, and a detection module 303.

[00107] The obtaining module 301 is configured to obtain target data submitted by a data submitter. The computing module 302 is configured to compute a data digest of the target data, and determine whether the computed data digest matches the data digest of the target data which has been recorded on the blockchain. The detection module 303 is configured to determine that the target data submitted by the data submitter is valid in response to that the computing module 302 determines the computed data digest matches the data digest of the target data which has been recorded on the blockchain; and determine that the target data submitted by the data submitter is invalid in response to that the computing module 302 determines that the computed data digest does not match the data digest of the target data which has been recorded on the blockchain.

[00108] In some embodiments, the terminal device includes a secure operation environment, and a private key corresponding to the terminal device is stored in the secure operation environment; the obtaining module 301 is further configured to: obtain a data digest of the target data submitted by the terminal device to the blockchain, the data digest being signed in the secure operation environment based on the private key of the terminal device; and the apparatus 30 further includes: a recordkeeping module 304 (not shown in FIG. 3), configured to verify the signature of the data digest based on a public key corresponding to the private key, and record the data digest of the target data in the blockchain in response to the signature being verified to be valid.

[00109] In some embodiments, the detection module 303 is configured to: verify, based on a preset verification algorithm, whether the computed data digest has been recorded in the blockchain; determine that the computed data digest matches the data digest of the target data which has been recorded on the blockchain in response to that it is verified that the computed data digest has been recorded in the blockchain; and determine that the computed data digest does not match the data digest of the target data which has been recorded on the blockchain

in response to that it is verified that the computed data digest is not recorded in the blockchain.

[00110] In some embodiments, the detection module 303 is configured to: obtain a data digest of the target data which has been recorded in the blockchain; determine whether the obtained data digest of the target data is the same as the computed data digest; and determine that the computed data digest matches the data digest of the target data which has been recorded on the blockchain in response to determining that the obtained data digest of the target data is the same as the computed data digest; and determine that the computed data digest does not match the data digest of the target data which has been recorded on the blockchain in response to determining that the obtained data digest of the target data is different from the computed data digest.

[00111] In some embodiments, description data of the target data is further recorded in the blockchain; and the detection module 303 is further configured to: in response to determining that the computed data digest matches the data digest of the target data which has been recorded on the blockchain, determine whether description data of the target data submitted by the data provider matches the description data of the target data recorded on the blockchain; and determine that the target data submitted by the data submitter is valid in response to determining that the description data of the target data submitted by the data provider matches the description data of the target data recorded on the blockchain.

[00112] In some embodiments, the description data includes: an acquisition time of the target data, an acquisition location of the target data, or an object related to the target data, or a combination thereof.

[00113] In some embodiments, the terminal device includes a body worn camera or an event data recorder. In addition, the target data includes video data, audio data, or image data, or a combination thereof, that are acquired by the body worn camera or the event data recorder as evidence or proof.

[00114] For details of the implementation of the functions and effects of each module in the foregoing apparatus, refer to the implementation of the corresponding steps in the foregoing methods. Details are not described herein again.

[00115] The apparatus embodiments are similar to the method embodiments. Therefore, for related parts, reference may be made to the descriptions in the method embodiments. The described apparatus embodiments is merely schematic. The modules described as separate

parts may or may not be physically separate, and the parts displayed as modules may or may not be physical modules, may be located in one position, or may be distributed on multiple network modules. Some or all of the modules may be selected according to actual needs to achieve the objectives of this specification. Those of ordinary skill in the art can understand and implement this specification without creative efforts.

[00116] The systems, apparatus or modules illustrated in the foregoing embodiments may be implemented by a computer chip or an entity, or implemented by a product having some function. A typical implementation device may be a computing device, and examples of the computing device may include a personal computer, a laptop computer, a cellular phone, a camera phone, a smartphone, a personal digital assistant, a media player, a navigation device, an email sending and receiving device, a game console, a tablet computer, or a wearable device, or a combination of any of these devices.

[00117] Similar to the foregoing method embodiments, this specification further provides embodiments of an electronic device. The electronic device includes: a processor and a memory configured to store machine executable instructions. The processor and the memory are usually interconnected through an internal bus. In other embodiments, the device may further include an external interface, so as to be able to communicate with other devices or components.

[00118] In some embodiments, by reading and executing machine executable instructions stored in the memory and corresponding to control logic for blockchain-based recordkeeping, the processor is caused to: obtain target data submitted by a data submitter; compute a data digest of the target data, and determine whether the computed data digest matches the data digest of the target data which has been recorded on the blockchain; and determine that the target data submitted by the data submitter is valid in response to determining that the computed data digest matches the data digest of the target data which has been recorded on the blockchain; and determine that the target data submitted by the data submitter is invalid in response to determining that the computed data digest does not match the data digest of the target data which has been recorded on the blockchain.

[00119] In some embodiments, the terminal device includes a secure operation environment, and a private key corresponding to the terminal device is stored in the secure operation environment; and by reading and executing machine executable instructions stored in the memory and corresponding to control logic for blockchain-based recordkeeping, the

processor is caused to: obtain a data digest of the target data submitted by the terminal device to the blockchain, the data digest being signed in the secure operation environment based on the private key corresponding to the terminal device to generate a signature; verify the signature of the data digest based on a public key corresponding to the private key; and record the data digest of the target data in the blockchain in response to the signature being verified to be valid.

[00120] In some embodiments, by reading and executing machine executable instructions stored in the memory and corresponding to control logic for blockchain-based recordkeeping, the processor is caused to: verify, based on a preset verification algorithm, whether the computed data digest has been recorded in the blockchain; determine that the computed data digest matches the data digest of the target data which has been recorded on the blockchain in response to that it is verified that the data digest has been recorded in the blockchain; and determine that the computed data digest does not match the data digest of the target data which has been recorded on the blockchain in response to that it is verified that the data digest is not recorded in the blockchain.

[00121] In some embodiments, by reading and executing machine executable instructions stored in the memory and corresponding to control logic for blockchain-based recordkeeping, the processor is caused to: obtain a data digest of the target data which has been recorded in the blockchain; determine whether the obtained data digest of the target data is the same as the computed data digest; and determine that the computed data digest matches the data digest of the target data which has been recorded on the blockchain in response to determining that the obtained data digest of the target data is the same as the computed data digest; and determine that the computed data digest does not match the data digest of the target data which has been recorded on the blockchain in response to determining that the obtained data digest of the target data is different from the computed data digest.

[00122] In some embodiments, description data of the target data is further recorded in the blockchain; and by reading and executing machine executable instructions stored in the memory and corresponding to control logic for blockchain-based recordkeeping, the processor is caused to: in response to determining that the computed data digest matches the data digest of the target data which has been recorded on the blockchain, determine whether description data of the target data submitted by the data provider matches the description data of the target data which has been recorded on the blockchain; and determine that the target data submitted by the data submitter is valid in response to determining that the description

data of the target data submitted by the data provider matches the description data of the target data which has been recorded on the blockchain.

[00123] Other embodiments of this specification will be obvious to those skilled in the art based on the specification disclosed herein. This specification is intended to cover any variations, uses, or adaptations of the embodiments following the general principles thereof and including such departures from this specification as come within known or customary practice in the art. The specification and examples are intended to be exemplary, with a scope and spirit of this specification being indicated by the following claims.

[00124] It will be appreciated that this specification is not limited to the exact constructions that have been described above and illustrated in the accompanying drawings. Various modifications and changes can be made without departing from the scope thereof. It is intended that the scope of this specification be limited by the appended claims.

[00125] The foregoing descriptions are some embodiments of this specification, and are not intended to limit this specification. Any modification, equivalent replacement, or improvement made within the spirit and principle of this specification shall fall within the protection scope of this specification.

Claims

1. A method for blockchain-based data verification, the method comprising:
 - obtaining, by a terminal device, target data submitted by a data submitter, wherein a private key of the terminal device is stored in a secure operation environment of the terminal device at a manufacturing stage of the terminal device, a first data digest of the target data is signed in the secure operation environment based on the private key to generate a signature, the signature is verified based on a public key corresponding to the private key, wherein the public key is owned by and received from a manufacturer of the terminal device and the first data digest of the target data is recorded in a blockchain in response to the signature being verified to be valid;
 - obtaining, by the terminal device, the first data digest of the target data from the blockchain;
 - computing, by the terminal device, a second data digest of the target data;
 - determining, by the terminal device, whether the second data digest matches the first data digest of the target data recorded in the blockchain; and
 - determining, by the terminal device, that the target data submitted by the data submitter is valid in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain.
2. The method according to claim 1, further comprising:
 - determining that the target data submitted by the data submitter is invalid in response to determining that the second data digest does not match the first data digest of the target data recorded in the blockchain.
3. The method according to claim 1, wherein the terminal device comprises a body worn camera or an event data recorder.
4. The method according to claim 3, wherein the target data comprises video data, audio data, or image data, or a combination thereof, which is acquired by the body worn camera or the event data recorder.
5. The method according to any one of the preceding claims, wherein determining whether the second data digest matches the first data digest of the target data recorded in the blockchain comprises:
 - verifying whether the second data digest has been recorded in the blockchain; and

determining that the second data digest matches the first data digest of the target data recorded in the blockchain in response to verifying that the second data digest has been recorded in the blockchain.

6. The method according to claim 5, wherein determining whether the second data digest matches the first data digest of the target data recorded in the blockchain further comprises:

determining that the second data digest does not match the first data digest of the target data recorded in the blockchain in response to verifying that the second data digest has not been recorded in the blockchain.

7. The method according to any one of the preceding claims, wherein determining whether the second data digest matches the first data digest of the target data recorded in the blockchain comprises:

obtaining the first data digest of the target data recorded in the blockchain;

determining whether the first data digest of the target data is the same as the second data digest; and

determining that the second data digest matches the first data digest of the target data recorded in the blockchain in response to determining that the first data digest of the target data is the same as the second data digest.

8. The method according to claim 7, wherein determining whether the second data digest matches the first data digest of the target data recorded in the blockchain further comprises:

determining that the second data digest does not match the first data digest of the target data recorded in the blockchain in response to determining that the first data digest of the target data is different from the second data digest.

9. The method according to any one of the preceding claims, wherein description data of the target data is recorded in the blockchain; and

determining that the target data submitted by the data submitter is valid in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain comprises:

in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain, determining whether description data of the target data submitted by the data submitter matches the description data of the target data recorded in the blockchain; and

determining that the target data submitted by the data submitter is valid in response to determining that the description data of the target data submitted by the data submitter matches the description data of the target data recorded in the blockchain.

10. The method according to claim 9, wherein the description data comprises: an acquisition time of the target data, an acquisition location of the target data, or an object related to the target data, or a combination thereof.

11. A system for blockchain-based data verification, comprising:
one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 10.

12. An apparatus for blockchain-based data verification, comprising a plurality of modules for performing the method of any of claims 1 to 10.

13. A non-transitory computer-readable storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform the method of any of claims 1 to 10.