

BLOCKCHAIN-BASED LOAN APPROVAL METHOD AND APPARATUS, NON-VOLATILE READABLE STORAGE MEDIUM, AND ELECTRONIC DEVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

5 The present application claims priority to the Chinese Patent Application No. 201811250030.2, filed on October 25, 2018 and entitled "BLOCKCHAIN-BASED LOAN APPROVAL METHOD AND APPARATUS, NON-VOLATILE READABLE STORAGE MEDIUM, AND ELECTRONIC DEVICE", which is incorporated herein by reference in its entirety.

10 TECHNICAL FIELD

 The present application relates to the field of computer technologies, and in particular to a blockchain-based loan approval method, a blockchain-based loan approval apparatus, a non-volatile readable storage medium, and an electronic device.

BACKGROUND

15 A loan manager is a business person serving a loan platform, whose main task is to assist a loan applicant in submitting application information to the loan platform, thereby completing approval and issuance of a loan. The inventor of the present application realizes that a widely shared credit evaluation system for a loan manager is lacked in the prior art and the loan manager cannot be ranked reliably. Moreover, even if a loan manager blacklist is created on the
20 loan platform, it only restricts frauds committed by the loan manager on a few loan platforms that reach a consensus, but cannot prevent the manager from maliciously implementing fraudulent loans on other loan platforms. In addition, an existing credit record of a loan manager is easily tampered with. Credibility of the credit record is not high, and a relative high fraud risk still exists.

25 It should be noted that the information disclosed in the background technology part is only used to enhance an understanding of the background of the present application, and therefore may include information that does not constitute prior art known to a person of ordinary skill in the art.

Technical Solutions

30 The present application provides a blockchain-based loan approval method, a blockchain-based loan approval apparatus, a non-volatile readable storage medium, and an

electronic device, thereby at least to a certain degree overcoming one or more technical problems caused by a limitation and a defect of a related technology.

According to an aspect of the present application, a blockchain-based loan approval method is provided, which is applied to a blockchain network storing credit authentication information of a loan manager, and the method includes:

receiving a loan approval request sent by the loan manager;

obtaining identity authentication information of the loan manager from the loan approval request;

obtaining the credit authentication information associated with the identity authentication information from the blockchain network; and

generating loan approval information based on the credit authentication information, where the loan approval information includes a loan approval result for the loan approval request.

According to an aspect of the present application, a blockchain-based loan approval apparatus is provided, including:

a receiving module, configured to receive a loan approval request sent by a loan manager;

a first obtaining module, configured to obtain identity authentication information of the loan manager from the loan approval request;

a second obtaining module, configured to obtain credit authentication information associated with the identity authentication information from a blockchain network; and

an approval module, configured to generate loan approval information based on the credit authentication information, where the loan approval information includes a loan approval result for the loan approval request.

According to an aspect of the present application, a non-volatile readable storage medium storing computer-readable instructions are provided, where the computer-readable instructions are executed by a processor to implement any one of the foregoing blockchain-based loan approval methods.

According to an aspect of the present application, an electronic device is provided, including: a memory, configured to store executable instructions; and a processor, configured to execute the executable instructions stored in the memory, where the processor is configured to perform any one of the foregoing blockchain-based loan approval methods by executing the

executable instructions.

Beneficial effects

5 In the loan approval method provided in the embodiments of the present application, a blockchain technology is used to store the identity authentication information of the loan manager, and the identity authentication information of the loan manager is mapped to the credit authentication information of the loan manager. When the loan application request sent by the loan manager is received, the credit authentication information of the loan manager can be obtained by verifying the identity authentication information of the loan manager, to provide a credit approval credential for a financial institution, thereby facilitating identification of a loan application with a fraud risk, and reducing a loan risk and a bad debt rate.

It should be understood that the foregoing general description and the following detailed description are merely illustrative and explanatory and do not limit the present application.

BRIEF DESCRIPTION OF DRAWINGS

15 The accompanying drawings herein are incorporated into the specification and form a part of the present specification, show the embodiments in accordance with the present application, and are used together with the specification to explain the principles of the present application. Obviously, the accompanying drawings in the following description are merely some embodiments of the present application. A person of ordinary skill in the art can derive other drawings from these accompanying drawings without creative efforts.

20 FIG. 1 schematically illustrates a flowchart of steps of a blockchain-based loan approval method in an example implementation of the present application;

FIG. 2 schematically illustrates a flowchart of some steps of a blockchain-based loan approval method in another example implementation of the present application;

25 FIG. 3 schematically illustrates a flowchart of some steps of a blockchain-based loan approval method in another example implementation of the present application;

FIG. 4 schematically illustrates a flowchart of some steps of a blockchain-based loan approval method in another example implementation of the present application;

FIG. 5 schematically illustrates a flowchart of some steps of a blockchain-based loan approval method in another example implementation of the present application;

30 FIG. 6 schematically illustrates a flowchart of some steps of a blockchain-based loan approval method in another example implementation of the present application;

FIG. 7 schematically illustrates a flowchart of some steps of a blockchain-based loan approval method in another example implementation of the present application;

FIG. 8 schematically illustrates a composition block diagram of a blockchain-based loan approval apparatus in an example implementation of the present application;

5 FIG. 9 schematically illustrates a schematic diagram of a program product in an example implementation of the present application; and

FIG. 10 schematically illustrates a schematic diagram of modules of an electronic device in an example implementation of the present application.

Embodiments of the invention

10 Example embodiments now are comprehensively described with reference to the accompanying drawings. However, the example embodiments can be implemented in a plurality of forms and should not be construed as limitations to the examples set forth herein. On the contrary, by providing these embodiments, the present application is more comprehensive and complete and a concept of example embodiments is comprehensively conveyed to a person
15 skilled in the art. The described features, structures, or characteristics may be combined in one or more embodiments in any suitable manner.

In addition, a drawing is only a schematic illustration of the present application and is not necessarily drawn in scale. A same reference numeral in the figure represents a same or similar part, so repeated descriptions of the parts are omitted. Some of the block diagrams shown in the
20 drawings are functional entities and do not necessarily correspond to physically or logically independent entities. These functional entities may be implemented in a software form, or in one or more hardware modules or integrated circuits, or in different networks and/or processor devices and/or micro controller devices.

In an example implementation of the present application, a blockchain-based loan approval
25 method is first provided, and is applied to a blockchain network storing credit authentication information of a loan manager. The blockchain network involves a plurality of blockchain nodes, and each of the blockchain nodes can correspond to a loan platform or a server with loan approval permission. In the blockchain network of the present application, each block on a blockchain stores credit authentication information of a specific quantity of loan managers, and
30 data stored on each block is real data that is agreed upon by all or some of the blockchain nodes.

As shown in FIG. 1, the blockchain-based loan approval method provided in the present example implementation may mainly include the following steps.

Step S110. Receive a loan approval request sent by the loan manager.

After obtaining relevant application information from a loan applicant, the loan manager may form a loan approval request in a specified format based on the specific application information, and submit the loan approval request to a corresponding loan platform for approval.

5 The loan platform may be a separate blockchain node in the blockchain network, or may be a set of a plurality of blockchain nodes (corresponding to servers with approval permission), or may be a non-blockchain node that can communicate with a blockchain node. No specific limitation is imposed on the present example implementation.

10 Step S120. Obtain identity authentication information of the loan manager from the loan approval request.

Based on the loan approval request received in step S110, the identity authentication information of the loan manager can be obtained from the loan approval request in the present step. The identity authentication information may include a plurality types of information related to an occupation of the loan manager such as a name, an ID number, and contact information of
15 the loan manager. The identity authentication information may be used to uniquely determine an identity of the loan manager.

Step S130. Obtain the credit authentication information associated with the identity authentication information from the blockchain network.

20 The credit authentication information of the loan manager is stored in the blockchain network. Therefore, based on the identity authentication information obtained in step S120, the credit authentication information associated with the identity authentication information can be obtained from the blockchain network. The credit authentication information may include credit rating information prepared for the loan manager according to a specific credit authentication rule, and may also include a loan application and approval record handled by the loan manager
25 as an agent.

Step S140. Generate loan approval information based on the credit authentication information, where the loan approval information includes a loan approval result for the loan approval request.

30 The credit authentication information for the loan manager is similar to a personal credit report provided by the Credit Reference Center of the People's Bank of China, and can truthfully record a practice credit history of the loan manager. Based on the credit authentication information obtained in step S130, the corresponding loan approval information may be

generated in the present step. The loan approval information includes the loan approval result for the loan approval request. It should be noted that the loan approval result is only a preliminary approval result provided based on the credit authentication information of the loan manager. An approval indicates that a credit status of the loan manager is good, and a final approval result needs to be provided based on specific application information of the loan applicant.

In the loan approval method provided in this implementation of the present application, a blockchain technology is used to store the identity authentication information of the loan manager, and the identity authentication information of the loan manager is mapped to the credit authentication information of the loan manager. When the loan application request sent by the loan manager is received, the credit authentication information of the loan manager can be obtained by verifying the identity authentication information of the loan manager, to provide a credit approval credential for a financial institution, thereby facilitating identification of a loan application with a fraud risk, and reducing a loan risk and a bad debt rate.

As shown in FIG. 2, based on the foregoing embodiment, after generating the loan approval information based on the credit authentication information in step S140, the loan approval method may further include the following steps.

Step S210. Update the credit authentication information of the loan manager based on the loan approval information.

Based on the loan approval information generated in step S140, the credit authentication information of the loan manager may be updated in the present step. For example, a new loan application record and an approval result of the loan application may be added to the credit certification information.

Step S220. Associate updated credit authentication information with the identity authentication information of the loan manager and broadcast the updated credit authentication information to the blockchain network.

After the credit authentication information of the loan manager is updated in step S210, the updated credit authentication information is associated with the identity authentication information of the loan manager and associated data is broadcast to the blockchain network in the present step. Afterwards, the associated data may be agreed upon by a plurality of blockchain nodes in the blockchain network and can be saved on the blockchain by reaching a consensus.

By using the blockchain network to store the credit authentication information of the loan manager, the latest credit authentication information of the loan manager can be obtained in real time, and data stored in the blockchain network features tamper-resistance. Therefore, credibility of the credit authentication information of the loan manager can be improved and a loan approval risk can be reduced.

In another example implementation of the present application, step S220 in which the updated credit authentication information is associated with the identity authentication information of the loan manager and is broadcast to the blockchain network may further include the following steps shown in FIG. 3.

Step S310. Associate the updated credit authentication information with the identity authentication information of the loan manager and save the updated credit authentication information in a block body of a current block.

In the blockchain network of the present application, each block includes two data storage areas: a block header and a block body. The block body is configured to store all credit authentication information recorded in the current block. In the present step, the updated credit authentication information may be associated with the identity authentication information of the loan manager, and the credit authentication information is saved in the block body of the current block. The block header is used to store information about a link between the current block and a previous block. All blocks can be linked one by one by using data stored in the block header to form a complete blockchain.

Step S320. When a preset condition is satisfied, obtain block header data of a previous block in the blockchain network, and obtain a parent block hash value through calculation based on the block header data.

When the preset condition is satisfied, the block header data of the previous block (namely, a new block generated recently) in the blockchain network can be obtained, and the parent block hash value can be obtained through calculation based on the block header data in the present step. For example, the SHA256 algorithm can be used to perform a hash operation on the block header data of the previous block to obtain a hash value as the parent block hash value of the current block. The preset condition in the present step may be either of the following: a time period from generation of the previous block reaches a preset time threshold; and an amount of the data stored in the block body of the current block reaches a preset data amount. The preset condition may alternatively be any other preset condition used to trigger generation of a new block. No specific limitation is imposed on the present example implementation.

Step S330. Calculate a block body hash value of the current block based on data stored in the block body of the current block.

The credit authentication information updated based on loan approval requests initiated by the loan manager over a period of time is stored in the block body of the current block. Based on the data stored in the block body, a hash value may be obtained and used as the block body hash value of the current block in the present step. For example, all credit certification information in the block body may be stored in the block body in a form of a Merkle tree. Specifically, a hash value uniquely related to the credit authentication information may be obtained after a hash operation is performed on each piece of credit authentication information, and the hash value is stored in a leaf node of the Merkle tree. Hash values stored in every two adjacent leaf nodes are combined, and a hash operation is performed again to obtain a hash value to be stored in one sub-node. A hash value of a root node can be finally obtained by performing a hash operation on every two hash values stored in sub-nodes from lower layers to upper layers. The hash value of the root node can be used as the block body hash value of the current block.

Step S340. Save the parent block hash value, the block body hash value, and a time stamp of current time in a block header of the current block.

After the parent block hash value and the block body hash value are respectively obtained through calculation in step S320 and step S330, a time stamp may be generated based on the current time in the present step. The time stamp is used to record a generation time of the current block. Then, the parent block hash value, the block body hash value, and the time stamp of the current time may be saved in the block header of the current block.

Step S350. Broadcast the current block to the blockchain network.

After the block header data is saved, the current block is broadcast to the blockchain network in the present step. In other words, the current block is added to the blockchain to add the credit authentication information of the loan manager into the blockchain. After a consensus is reached, the current block may be saved to all or some of the blockchain nodes in the blockchain network and a new block may be generated.

As shown in FIG. 4, based on the foregoing example implementations, step S120 in which the identity authentication information of the loan manager is obtained from the loan approval request may include the following steps.

Step S410. Obtain a public key and a digital signature from the loan approval request, where the digital signature is obtained through encryption by using a private key corresponding

to the public key.

In the present example implementation, the loan approval request received in step S110 includes the public key and the digital signature. Each loan manager may hold a key pair consisting of a public key and a private key. When initiating a loan approval request, the loan manager may first perform a hash operation on relevant information in the loan approval request to obtain a digital digest, and encrypt the digital digest by using the respective private key to obtain a corresponding digital signature.

Step S420. Verify whether the digital signature is valid by using the public key.

Based on the public key and the digital signature obtained in step S410, authenticity of the loan approval request can be verified in the present step. A specific verification method may include, for example, first decrypting the digital signature by using the public key to obtain a digital digest to be verified; performing a hash operation on the relevant information in the loan approval request by using the same hash algorithm as the encryption process to obtain an original digital digest; and determining, through comparison, whether the digital digest to be verified is the same as the original digital digest. If a comparison result is that the hash values of the two digests are the same, the digital signature can be considered valid. If the comparison result is that the hash values of the two digests are different, the digital signature can be considered invalid.

Step S430. Obtain the identity authentication information of the loan manager from the loan approval request when the digital signature is verified to be valid.

Based on a verification result in step S420, the identity authentication information of the loan manager may be obtained from the loan approval request in the present step when the digital signature is verified to be valid. If the digital signature is verified to be invalid in step S420, it can be considered that the loan manager initiating the loan approval request is suspected to fraudulently use identity information of another loan manager. Afterwards, an identity of the loan manager may be verified by another means, and an approval process of the current loan approval request may continue.

In the present example implementation, using a digital signature to verify the identity of the loan manager through asymmetric encryption can prevent the loan manager from fraudulently using an identity of another person to apply for a loan, thereby improving credibility of a loan approval method.

As shown in FIG. 5, in another example implementation of the present application, step

S130 in which the credit authentication information associated with the identity authentication information is obtained from the blockchain network may mainly include the following steps.

Step S510. Obtain node information of a preset quantity of blockchain nodes from the blockchain network.

5 In the present step, the node information of the preset quantity of blockchain nodes can be first obtained from the blockchain network according to a specific rule. Each blockchain node corresponding to the node information should be a node that stores a complete blockchain.

Step S520. Obtain, based on the node information, the credit authentication information associated with the identity authentication information from the blockchain nodes.

10 Because each of the blockchain nodes corresponding to the node information stores the complete blockchain, a plurality of pieces of the credit authentication information associated with the identity authentication information may be obtained from the corresponding blockchain nodes in the present step.

Step S530. Determine whether the credit authentication information obtained from each of
15 the blockchain nodes is consistent.

In the present step, the plurality of pieces of the obtained credit authentication information can be compared to determine whether the credit authentication information stored on each of the blockchain nodes is consistent.

Step S540. When the credit authentication information is consistent, use the credit
20 authentication information as valid credit authentication information of the loan manager.

Through consistency comparison, the authenticity and credibility of the credit authentication information can further be confirmed, and security of the loan approval method can be improved.

As shown in FIG. 6, in another example implementation of the present application, after
25 step S130 in which the credit authentication information associated with the identity authentication information is obtained from the blockchain network, the loan approval method may further include the following steps.

Step S610. Obtain a target image based on the identity authentication information, where the target image is a real facial image of the loan manager.

30 In the present step, after the identity authentication information of the loan manager is obtained, the target image corresponding to the loan manager can be obtained based on the

identity authentication information. The target image is a real facial image of the loan manager stored in a blockchain node.

Step S620. Collect a current facial image of the loan manager, and normalize the current facial image based on the target image to obtain a standard facial image.

5 In the present step, when the loan manager submits the loan approval request, the current facial image of the loan manager is collected, and is normalized based on a feature of the target image to obtain the standard facial image. Normalization may include, for example, normalizing a plurality of features such as background, angle, size, and color. Normalization can minimize interference caused by irrelevant feature information other than a facial feature to two images.

10 Step S630. Input the standard facial image and the target image into a pre-trained convolutional neural network-based image comparison model to obtain image similarity.

In the present step, an image comparison model based on a convolutional neural network is pre-trained, and the standard facial image and the target image are input into the image comparison model to obtain the image similarity of the two images.

15 Step S640. When the image similarity is greater than a preset threshold, determine that the identity authentication information of the loan manager is true.

By comparing the image similarity obtained in step S630 with the preset threshold, authenticity of the identity authentication information of the loan manager can be determined in the present step. For example, if the preset threshold is set to 80% and the image similarity
20 obtained in step S630 is 85%, it can be determined that the identity authentication information used by the loan manager that submits the loan approval request is true.

In addition to verifying identity authenticity through facial recognition, the present example implementation may extract micro-expression features at a specific position (for example, eyes or mouth) of the standard facial image. The micro-expression features include a shape feature
25 and a texture feature. Subsequently, the micro-expression features are compared with a micro-expression image in a preset micro-expression image library. A fraud risk coefficient is obtained based on a comparison result. A micro-expression technology is used to determine the loan manager's personal status existing when the loan approval request is submitted and to obtain the fraud risk coefficient through calculation. In this way, more reference basis can be
30 provided for a loan approval and a fraud risk can be reduced.

As shown in FIG. 7, in another example implementation of the present application, after step S140 in which the loan approval information is generated based on the credit authentication

information, the loan approval method may further include the following steps:

Step S710. Receive an appeal request sent by the loan manager for the loan approval result.

If the approval result of the current loan approval request indicates "failed", the loan manager may initiate the appeal request. The appeal request may include a specific appeal
5 reason of the loan manager.

Step S720. Generate an appeal result based on the appeal request and update the credit authentication information of the loan manager based on the appeal result.

After the specific appeal reason is reviewed, based on the appeal request sent by the loan manager, the appeal result is generated and the credit authentication information of the loan
10 manager is updated based on the appeal result in the present step.

Step S730. Associate updated credit authentication information with the identity authentication information of the loan manager and broadcast the updated credit authentication information to the blockchain network.

Similar to the loan approval result, the credit certification information updated based on the
15 appeal result is also broadcast to the blockchain network and stored by blockchain nodes within the blockchain network in a distributed way.

It should be noted that, although the foregoing example implementations describe steps of the methods in the present application in a particular sequence, it does not require or imply that these steps necessarily be performed in that particular sequence, or that all steps necessarily be
20 performed to achieve a desired result. Additionally or alternatively, some steps may be omitted, a plurality of steps may be combined into one step for execution, and/or a step may be broken down into a plurality of steps for execution, or the like.

In an example implementation of the present application, a blockchain-based loan approval apparatus is also provided. As shown in FIG. 8, a loan approval apparatus 800 may mainly
25 include a receiving module 810, a first obtaining module 820, a second obtaining module 830, and an approval module 840. The receiving module 810 is configured to receive a loan approval request sent by a loan manager. The first obtaining module 820 is configured to obtain identity authentication information of the loan manager from the loan approval request. The second obtaining module 830 is configured to obtain credit authentication information associated with
30 the identity authentication information from a blockchain network. The approval module 840 is configured to generate loan approval information based on the credit authentication information, where the loan approval information includes a loan approval result for the loan approval

request.

The loan approval apparatus 800 may further include:

a first update module, configured to update the credit authentication information of the loan manager based on the loan approval information; and

- 5 a first broadcast module, configured to associate updated credit authentication information with the identity authentication information of the loan manager and broadcast the updated credit authentication information to the blockchain network.

The first broadcast module may further include:

- 10 a first saving unit, configured to associate the updated credit authentication information with the identity authentication information of the loan manager and save the updated credit authentication information in a block body of a current block;

a first calculation unit, configured to: when a preset condition is satisfied, obtain block header data of a previous block in the blockchain network, and obtain a parent block hash value through calculation based on the block header data;

- 15 a second calculation unit, configured to calculate a block body hash value of the current block based on data stored in the block body of the current block;

a second saving module, configured to save the parent block hash value, the block body hash value, and a time stamp of current time in a block header of the current block; and

a broadcast unit, configured to broadcast the current block to the blockchain network.

- 20 The first obtaining module 820 may include:

a first obtaining unit, configured to obtain a public key and a digital signature from the loan approval request, where the digital signature is obtained through encryption by using a private key corresponding to the public key;

- 25 a verification unit, configured to verify whether the digital signature is valid by using the public key; and

a second obtaining unit, configured to obtain the identity authentication information of the loan manager from the loan approval request when the digital signature is verified to be valid.

The second obtaining module 830 may include:

a third obtaining unit, configured to obtain node information of a preset quantity of

blockchain nodes from the blockchain network;

a fourth obtaining unit, configured to obtain, based on the node information, the credit authentication information associated with the identity authentication information from each of the blockchain nodes;

5 a determining unit, configured to determine whether the credit authentication information obtained from each of the blockchain nodes is consistent; and

an association unit, configured to: when the credit authentication information is consistent, use the credit authentication information as valid credit authentication information of the loan manager.

10 The loan approval apparatus 800 may further include:

a facial image obtaining module, configured to obtain a target image based on the identity authentication information, where the target image is a real facial image of the loan manager;

a facial image collection module, configured to: collect a current facial image of the loan manager, and normalize the current facial image based on the target image to obtain a standard
15 facial image;

a facial image processing module, configured to input the standard facial image and the target image into a pre-trained convolutional neural network-based image comparison model to obtain image similarity; and

20 a judgment module, configured to, when the image similarity is greater than a preset threshold, determine that the identity authentication information of the loan manager is true.

The loan approval apparatus 800 may further include:

a second receiving modul, configured to receive an appeal request sent by the loan manager for the loan approval result;

25 a second update module, configured to generate an appeal result based on the appeal request and update the credit authentication information of the loan manager based on the appeal result; and

a second broadcast module, configured to associate updated credit authentication information with the identity authentication information of the loan manager and broadcast the updated credit authentication information to the blockchain network.

30 Specific details of the foregoing blockchain-based loan approval apparatus are already

described in detail in the corresponding blockchain-based loan approval method. Therefore, details are not described herein again.

It should be noted that although several modules or units of a device for action execution are mentioned in the foregoing detailed description, such division is not mandatory. In fact, according to implementations of the present application, the features and functions of the two or more modules or units described above may be embodied in one module or unit. On the contrary, a feature and a function of one module or unit described above may be further divided into a plurality of modules or units and be embodied.

In an example implementation of the present application, a non-volatile readable storage medium storing computer-readable instructions is further provided. When executed by a processor, the computer-readable instructions can implement the foregoing blockchain-based loan approval method of the present application. In some possible implementations, aspects of the present application may also be implemented as a form of program product, which includes program code. The program product may be stored in a non-volatile readable storage medium (which may be a CD-ROM, a USB drive, a removable hard disk, or the like) or on a network. When the program product is run on a computing device (which may be a personal computer, a server, a terminal apparatus, a network device, or the like), the program code is used to enable the computing device to perform the methods and steps in the foregoing example implementations of the present application.

As shown in FIG. 9, a program product 900 used to implement the foregoing methods according to implementations of the present application may use a portable compact disk read-only memory (CD-ROM) and include program code and may be run on a computing device (for example, a personal computer, a server, a terminal apparatus, or a network device). However, the program product of the present application is not limited thereto. In the present example implementation, the non-volatile readable storage medium may be any tangible medium containing or storing a program. The program may be used by or in combination with an instruction execution system, apparatus, or device.

The program product may be any combination of one or more readable media. The readable medium may be a readable signal medium or a non-volatile readable storage medium.

The non-volatile readable storage medium may be, as an example but not limited to, an electrical, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus or component, or any combination thereof. A more specific example (non-exhaustive list) of the non-volatile readable storage medium includes an electrical connection with one or more leads,

a portable disk, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or flash), an optical fiber, a portable compact disk read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the above.

5 The readable signal medium may include a data signal that is propagated in a baseband or as a part of a carrier, and carries readable program code. Such propagated data signal may take a plurality of forms, including but not limited to an electromagnetic signal, an optical signal, or any suitable combination of the above. The readable signal medium may also be any readable medium other than the non-volatile readable storage medium. The readable medium may send,
10 propagate, or transmit a program for use by or in combination with an instruction execution system, apparatus, or component.

The program code included in the readable medium may be transmitted in any suitable medium, including but not limited to a wireless medium, a wired medium, an optical cable, RF, or the like, or any suitable combination of the above.

15 Program code for executing an operation of the present application may be written in one or any combination of a plurality of program design languages. The program design languages include object-oriented program design languages such as Java, C ++, and the like, and a conventional procedural program design language such as C or a similar program design language. The program code may be executed entirely on a user computing device, partly on a
20 user computing device, as a separate software package, partly on a user computing device and partly on a remote computing device, or entirely on a remote computing device or server. In a case involving a remote computing device, the remote computing device may be connected to a user computing device through any type of network (including a local area network (LAN), a wide area network (WAN), or the like). Alternatively, the remote computing device may be
25 connected to an external computing device, for example, by using an Internet service provider for connection over the Internet.

In an example implementation of the present application, an electronic device is further provided. The electronic device includes: a memory, configured to store executable instructions; and a processor, configured to execute the executable instructions stored in the memory. The
30 processor is configured to execute the executable instructions to perform the methods and steps of the foregoing example embodiments in the present application.

An electronic device 1000 in an example implementation is described below with reference to FIG. 10. The electronic device 1000 is merely an example and shall not impose any limitation

on a functionality and a scope of use of the embodiments of the present application.

As shown in FIG. 10, the electronic device 1000 is represented as a general-purpose computing device. Components of the electronic device 1000 may include but are not limited to at least one processing unit 1010, at least one storage unit 1020, a bus 1030 connecting different system components (including the processing unit 1010 and the storage unit 1020), and a display unit 1040.

The storage unit 1020 stores program code and the program code may be executed by the processing unit 1010, so that the processing unit 1010 performs the methods and steps in the foregoing example implementations of the present application.

The storage unit 1020 may include a readable medium in a form of a volatile storage unit, such as a random access memory (RAM) unit 1021 and/or a cache memory unit 1022, and may further include a read-only memory (ROM) unit 1023.

The storage unit 1020 may also include a program/utility 1024 with a set (at least one) of program modules 1025. Such program modules include but are not limited to an operating system, one or more applications, another program module, and program data. Each or a combination of these examples may include an implementation of a network environment.

The bus 1030 may be one or more of several types of bus structures, including a memory unit bus or a memory unit controller, a peripheral bus, a graphics acceleration port, a processing unit, or a local bus using any of various bus structures.

The electronic device 1000 may also communicate with one or more external devices 1100 (for example, a keyboard, a pointing device, a Bluetooth device), with one or more devices that enable a user to interact with the electronic device 1000, and/or with any device (for example, a router or a modem) that enables the electronic device 1000 to communicate with one or more other computing devices. Such communication can be performed by using an input/output (I/O) interface 1050. In addition, the electronic device 1000 may communicate with one or more networks (such as a local area network (LAN), a wide area network (WAN), and/or a public network such as the Internet) by using a network adapter 1060. As shown in FIG. 10, the network adapter 1060 may communicate with other modules of the electronic device 1000 through the bus 1030. It should be understood that, although not shown in the figures, other hardware and/or software modules may be used in combination with the electronic device 1000, including but not limited to microcode, a device drive, a redundancy processing unit, an external disk drive array, a RAID system, a tape drive, a data backup storage system, and the like.

A person skilled in the art should understand that aspects of the present application may be implemented as systems, methods, or program products. Therefore, the aspects of the present application may be specifically implemented in the following manners, that is, a hardware-only implementation, a software-only implementation (including firmware, microcode, and the like),
5 or a implementation in which hardware and software are combined, which may be collectively referred to as "circuit", "module" or "system".

After considering the specification and practicing the invention disclosed herein, a person skilled in the art easily figures out other implementation solutions of the present application. The present application is intended to cover any variations, functions, or adaptive changes of the
10 present application. These variations, functions, or adaptive changes comply with general principles of the present application, and include common knowledge or a commonly used technical means in the technical field that is not disclosed in the present application. The specification and the embodiments are merely considered as examples, and the actual scope and the spirit of the present application are specified by the appended claims.

15 The features, structures, or characteristics described above may be combined in one or more implementations in any suitable manner. If possible, the features discussed in the embodiments are interchangeable. In the foregoing description, many specific details are provided to give sufficient understanding of the implementations of the present application. However, a person skilled in the art should be aware that the technical solutions in the present
20 application may be implemented without one or more of the specific details, or by using another method, component, material, or the like. In other cases, known structures, materials, or operations are not shown or described in detail to avoid blurring the aspects of the present application.

CLAIMS

What is claimed is:

1. A blockchain-based loan approval method, applied to a blockchain network storing credit authentication information of a loan manager, wherein the method comprises:

receiving a loan approval request sent by the loan manager;

obtaining identity authentication information of the loan manager from the loan approval request;

obtaining the credit authentication information associated with the identity authentication information from the blockchain network; and

generating loan approval information based on the credit authentication information, wherein the loan approval information includes a loan approval result for the loan approval request;

wherein the obtaining identity authentication information of the loan manager from the loan approval request comprises:

obtaining a public key and a digital signature from the loan approval request, wherein the digital signature is obtained through encryption by using a private key corresponding to the public key;

verifying whether the digital signature is valid by using the public key; and

obtaining the identity authentication information of the loan manager from the loan approval request when the digital signature is verified to be valid.

2. The blockchain-based loan approval method according to claim 1, wherein after the generating loan approval information based on the credit authentication information, the method further comprises:

updating the credit authentication information of the loan manager based on the loan approval information; and

associating updated credit authentication information with the identity authentication information of the loan manager and broadcasting the updated credit authentication information to the blockchain network.

3. The blockchain-based loan approval method according to claim 2, wherein the associating updated credit authentication information with the identity authentication

information of the loan manager and broadcasting the updated credit authentication information to the blockchain network comprises:

associating the updated credit authentication information with the identity authentication information of the loan manager and saving the updated credit authentication information in a block body of a current block;

when a preset condition is satisfied, obtaining block header data of a previous block in the blockchain network, and obtaining a parent block hash value through calculation based on the block header data;

calculating a block body hash value of the current block based on data stored in the block body of the current block;

saving the parent block hash value, the block body hash value and a time stamp of current time in a block header of the current block; and

broadcasting the current block to the blockchain network.

4. The blockchain-based loan approval method according to claim 1, wherein the obtaining the credit authentication information associated with the identity authentication information from the blockchain network comprises:

obtaining node information of a preset quantity of blockchain nodes from the blockchain network;

obtaining, based on the node information, the credit authentication information associated with the identity authentication information from each of the blockchain nodes;

determining whether the credit authentication information obtained from each of the blockchain nodes is consistent; and

when the credit authentication information is consistent, using the credit authentication information as valid credit authentication information of the loan manager.

5. The blockchain-based loan approval method according to claim 1, wherein after the obtaining identity authentication information of the loan manager from the loan approval request, the method further comprises:

obtaining a target image based on the identity authentication information, wherein the target image is a real facial image of the loan manager;

collecting a current facial image of the loan manager, and normalizing the current facial image based on the target image to obtain a standard facial image;

inputting the standard facial image and the target image into a pre-trained convolutional neural network-based image comparison model to obtain image similarity; and

when the image similarity is greater than a preset threshold, determining that the identity authentication information of the loan manager is true.

6. The blockchain-based loan approval method according to claim 1, wherein after the generating loan approval information based on the credit authentication information, the method further comprises:

receiving an appeal request sent by the loan manager for the loan approval result;

generating an appeal result based on the appeal request and updating the credit authentication information of the loan manager based on the appeal result; and

associating updated credit authentication information with the identity authentication information of the loan manager and broadcasting the updated credit authentication information to the blockchain network.

7. A blockchain-based loan approval apparatus, comprising:

a receiving module, configured to receive a loan approval request sent by a loan manager;

a first obtaining module, configured to obtain identity authentication information of the loan manager from the loan approval request;

a second obtaining module, configured to obtain credit authentication information associated with the identity authentication information from a blockchain network; and

an approval module, configured to generate loan approval information based on the credit authentication information, wherein the loan approval information comprises a loan approval result for the loan approval request;

wherein the first obtaining module includes:

a first obtaining unit, configured to obtain a public key and a digital signature from the loan approval request, where the digital signature is obtained through encryption by using a private key corresponding to the public key;

a verification unit, configured to verify whether the digital signature is valid by using the public key; and

a second obtaining unit, configured to obtain the identity authentication information of the loan manager from the loan approval request when the digital signature is verified to be valid.

8. A non-volatile readable storage medium on which computer-readable instructions are stored, wherein when the computer-readable instructions are executed by a processor, the processor is configured to:

receive a loan approval request sent by a loan manager;

obtain identity authentication information of the loan manager from the loan approval request;

obtain credit authentication information associated with the identity authentication information from a blockchain network; and

generate loan approval information based on the credit authentication information, wherein the loan approval information comprises a loan approval result for the loan approval request;

wherein when the computer-readable instructions are executed by the processor, the processor is configured to obtain the identity authentication information of the loan manager from the loan approval request by performing the following steps:

obtaining a public key and a digital signature from the loan approval request, wherein the digital signature is obtained through encryption by using a private key corresponding to the public key;

verifying whether the digital signature is valid by using the public key; and

obtaining the identity authentication information of the loan manager from the loan approval request when the digital signature is verified to be valid.

9. The non-volatile readable storage medium according to claim 8, wherein when the computer-readable instructions are executed by the processor, the processor is further configured to:

update the credit authentication information of the loan manager based on the loan approval information; and

associating updated credit authentication information with the identity authentication information of the loan manager and broadcasting the updated credit authentication information to the blockchain network.

10. The non-volatile readable storage medium according to claim 9, wherein when the computer-readable instructions are executed by the processor, the processor is configured to associate the updated credit authentication information with the identity authentication information of the loan manager and broadcast the updated credit authentication information to the blockchain network by performing the following steps:

associating the updated credit authentication information with the identity authentication information of the loan manager and saving the updated credit authentication information in a block body of a current block;

when a preset condition is satisfied, obtaining block header data of a previous block in the blockchain network, and obtaining a parent block hash value through calculation based on the block header data;

calculating a block body hash value of the current block based on data stored in the block body of the current block;

saving the parent block hash value, the block body hash value and a time stamp of current time in a block header of the current block; and

broadcasting the current block to the blockchain network.

11. The non-volatile readable storage medium according to claim 8, wherein when the computer-readable instructions are executed by the processor, the processor is configured to obtain the credit authentication information associated with the identity authentication information from the blockchain network by performing the following steps:

obtaining node information of a preset quantity of blockchain nodes from the blockchain network;

obtaining, based on the node information, the credit authentication information associated with the identity authentication information from each of the blockchain nodes;

determining whether the credit authentication information obtained from each of the blockchain nodes is consistent; and

when the credit authentication information is consistent, using the credit authentication

information as valid credit authentication information of the loan manager.

12. The non-volatile readable storage medium according to claim 8, wherein when the computer-readable instructions are executed by the processor, the processor is further configured to:

obtain a target image based on the identity authentication information, wherein the target image is a real facial image of the loan manager;

collect a current facial image of the loan manager, and normalize the current facial image based on the target image to obtain a standard facial image;

inputting the standard facial image and the target image into a pre-trained convolutional neural network-based image comparison model to obtain image similarity; and

when the image similarity is greater than a preset threshold, determining that the identity authentication information of the loan manager is true.

13. The non-volatile readable storage medium according to claim 8, wherein when the computer-readable instructions are executed by the processor, the processor is further configured to:

receive an appeal request sent by the loan manager for the loan approval result;

generate an appeal result based on the appeal request and update the credit authentication information of the loan manager based on the appeal result; and

associating updated credit authentication information with the identity authentication information of the loan manager and broadcasting the updated credit authentication information to the blockchain network.

14. An electronic device, comprising:

a memory, configured to store executable instructions; and

a processor, configured to execute the executable instructions stored in the memory, wherein when executing the executable instructions, the processor is configured to perform the following steps:

receiving a loan approval request sent by a loan manager;

obtaining identity authentication information of the loan manager from the loan approval request;

obtaining the credit authentication information associated with the identity authentication information from a blockchain network; and

generating loan approval information based on the credit authentication information, wherein the loan approval information comprises a loan approval result for the loan approval request;

wherein when executing the executable instructions, the processor is configured to obtain the identity authentication information of the loan manager from the loan approval request by performing the following steps:

obtaining a public key and a digital signature from the loan approval request, wherein the digital signature is obtained through encryption by using a private key corresponding to the public key;

verifying whether the digital signature is valid by using the public key; and

obtaining the identity authentication information of the loan manager from the loan approval request when the digital signature is verified to be valid.

15. The electronic device according to claim 14, wherein when executing the executable instructions, the processor is configured to, after generating the loan approval information based on the credit authentication information, further perform the following steps:

updating the credit authentication information of the loan manager based on the loan approval information; and

associating updated credit authentication information with the identity authentication information of the loan manager and broadcasting the updated credit authentication information to the blockchain network.

16. The electronic device according to claim 15, wherein when executing the executable instructions, the processor is configured to associate the updated credit authentication information with the identity authentication information of the loan manager and broadcast the updated credit authentication information to the blockchain network by performing the following steps:

associating the updated credit authentication information with the identity authentication information of the loan manager and saving the updated credit authentication information in a block body of a current block;

when a preset condition is satisfied, obtaining block header data of a previous block in the blockchain network, and obtaining a parent block hash value through calculation based on the block header data;

calculating a block body hash value of the current block based on data stored in the block body of the current block;

saving the parent block hash value, the block body hash value and a time stamp of current time in a block header of the current block; and

broadcasting the current block to the blockchain network.

17. The electronic device according to claim 14, wherein when executing the executable instructions, the processor is configured to obtain the credit authentication information associated with the identity authentication information from the blockchain network by performing the following steps:

obtaining node information of a preset quantity of blockchain nodes from the blockchain network;

obtaining, based on the node information, the credit authentication information associated with the identity authentication information from each of the blockchain nodes;

determining whether the credit authentication information obtained from each of the blockchain nodes is consistent; and

when the credit authentication information is consistent, using the credit authentication information as valid credit authentication information of the loan manager.