

Description

KYC-BASED ANTI-MONEY-LAUNDERING METHOD AND APPARATUS BY MEANS OF BLOCK CHAIN, DEVICE, AND STORAGE MEDIUM

Technical Field

The present invention relates to the technical field of block chains, and in particular, to a KYC-based anti-money-laundering method by means of a block chain.

Background Art

Currently, a block chain is a novel application mode of computer technologies such as distributed data storage, point-to-point transmission, a consensus mechanism, and an encryption algorithm. The consensus mechanism is how all accounting nodes reach a consensus, to identify validity of a record, and this is not only a means for identification, but also is a means for preventing tampering.

With respect to a KYC (Know-your-customer) rule, in the existing financial transaction scenario, a customer identity needs to be learned, to make a KYC rule, so as to assess a customer risk, thereby avoiding illegal customers that perform money laundering and the like.

The foregoing existing technical solution has the following defect: costs on the know-your-customer rule are relatively high.

Summary of the Invention

The objective of the present invention is to provide a KYC-based anti-money-laundering method and apparatus by means of a block chain, a device, and a storage medium that save costs on a know-your-customer rule.

The foregoing inventive objective 1 of the present invention is achieved by using the following technical solution:

a KYC-based anti-money-laundering method by means of a block chain, wherein the KYC-based anti-money-laundering method by means of a block chain comprises: obtaining user identity information, and storing the user identity information into a third-party database by using a block chain; if user transaction information is obtained, obtaining the user identity information from the third-party database; and verifying the user identity information, and if verification succeeds, responding to the user transaction information.

By using the foregoing technical solution, user information is stored into the third-party database

by using a block chain technology, so that user identification information can be retrieved during financial transaction without separate costs, and identity identification is performed on the user. In addition, by using the block chain technology, the decentralization of the block chain technology, and the cryptography technology in the block chain technology are used, so that the user identity information cannot be tampered and falsified, and can only be updated, so as to ensure the authenticity of the user identity information, thereby providing technical support for combating money laundering.

The present invention is further set as follows: the obtaining user identity information, and storing the user identity information into a third-party database by using a block chain comprises:

the user identity information comprising a user identity and a user historical transaction record; and encrypting the user historical transaction record by using an asymmetric cryptographic algorithm, and storing the encrypted user historical transaction record into the third-party database.

Preferably, the encrypting the user historical transaction record by using an asymmetric cryptographic algorithm, and storing the encrypted user historical transaction record into the third-party database comprises:

each user historical transaction record comprising corresponding transaction time and transaction content; calculating each historical transaction record by using a Hash algorithm, to obtain a corresponding block and Hash value; forming the block corresponding to each historical transaction record into a block chain according to a sequence of the transaction time; and encrypting the block chain by using the asymmetric cryptographic algorithm, and storing the block chain into the third-party database according to the user identity.

Preferably, the forming the block corresponding to each historical transaction record into a block chain according to a sequence of the transaction time, and storing the block chain into the third-party database comprises:

calculating a first historical transaction record by using the Hash algorithm according to the sequence of the transaction time, to obtain a first block and a first Hash value; and calculating an Mth historical transaction record and an (M-1)th Hash value starting from a second historical transaction record by using the Hash algorithm, to obtain an Mth block and an Mth Hash value, and forming the first, second, ..., Mth blocks into the block chain, wherein M is a positive integer greater than or equal to 2.

By using the foregoing technical solution, the block chain uses a one-way Hash algorithm, and each newly generated block is strictly advanced in the timeline order. The irreversibility and the irrevocability of time cause any behavior that attempts to invade and tamper data information in the block chain to be easily traced, leading to rejection by other nodes, and extremely high costs of

fraud, so that related illegal behaviors can be limited. In addition, the block chain is encrypted by using the asymmetric cryptographic algorithm to ensure that the user identity information will not be leaked.

The present invention is further set as follows: the obtaining the user identity information from the third-party database if user transaction information is obtained comprises:

the asymmetric cryptographic algorithm comprising a public key and a private key; encrypting the block chain by using the public key, and storing the encrypted block chain into the third-party database; the user transaction information comprising the user identity, and obtaining, from the third-party database according to the user identity, the corresponding block chain after encryption; and decrypting, by using the private key, the corresponding block chain after encryption, to obtain the user identity information.

By using the foregoing technical solution, the user transaction information is encrypted and decrypted by using the public key and the private key, ensuring that the user transaction information is not leaked during the transmission and viewing process, thereby ensuring the security of the information.

The foregoing inventive objective 2 of the present invention is achieved by using the following technical solution:

a KYC-based anti-money-laundering apparatus by means of a block chain, wherein the KYC-based anti-money-laundering apparatus by means of a block chain comprises:

a first obtaining module, configured to: obtain user identity information, and store the user identity information into a third-party database by using a block chain; a second obtaining module, configured to: if user transaction information is obtained, obtain the user identity information from the third-party database; and a verification module, configured to: verify the user identity information, and if verification succeeds, respond to the user transaction information.

By using the foregoing technical solution, user information is stored into the third-party database by using a block chain technology, so that user identification information can be retrieved during financial transaction without separate costs, and identity identification is performed on the user. In addition, by using the block chain technology, the decentralization of the block chain technology, and the cryptography technology in the block chain technology are used, so that the user identity information cannot be tampered and falsified, and can only be updated, so as to ensure the authenticity of the user identity information, thereby providing technical support for combating money laundering.

The foregoing inventive objective 3 of the present invention is achieved by using the following technical solution:

a computer device, comprising a memory, a processor, and a computer program that is stored in

the memory and that can run on the processor, wherein when the processor executes the computer program, the steps of the KYC-based anti-money-laundering method by means of a block chain are implemented.

The foregoing inventive objective 4 of the present invention is achieved by using the following technical solution:

a computer readable storage medium, storing a computer program, wherein when the computer program is executed by a processor, the steps of the KYC-based anti-money-laundering method by means of a block chain are implemented.

In summary, the present invention has the following beneficial technical effects:

1. User information is stored into the third-party database by using a block chain technology, so that user identification information can be retrieved during financial transaction without separate costs, and identity identification is performed on the user; in addition, by using the block chain technology, the decentralization of the block chain technology, and the cryptography technology in the block chain technology are used, so that the user identity information cannot be tampered and falsified, and can only be updated, so as to ensure the authenticity of the user identity information, thereby providing technical support for combating money laundering.
2. The block chain uses a one-way Hash algorithm, and each newly generated block is strictly advanced in the timeline order. The irreversibility and the irrevocability of time cause any behavior that attempts to invade and tamper data information in the block chain to be easily traced, leading to rejection by other nodes, and extremely high costs of fraud, so that related illegal behaviors can be limited; and in addition, the block chain is encrypted by using the asymmetric cryptographic algorithm to ensure that the user identity information will not be leaked.
3. The user transaction information is encrypted and decrypted by using the public key and the private key, ensuring that the user transaction information is not leaked during the transmission and viewing process, thereby ensuring the security of the information.

Brief Description of the Drawings

FIG. 1 is a schematic diagram of an application environment of a KYC-based anti-money-laundering method by means of a block chain in an embodiment of the present invention;

FIG. 2 is a flowchart of a KYC-based anti-money-laundering method by means of a block chain in an embodiment of the present invention;

FIG. 3 is a flowchart of implementation of step S10 in a KYC-based anti-money-laundering method by means of a block chain in an embodiment of the present invention;

FIG. 4 is a flowchart of implementation of step S12 in a KYC-based anti-money-laundering

method by means of a block chain in an embodiment of the present invention;

FIG. 5 is a flowchart of implementation of step S124 in a KYC-based anti-money-laundering method by means of a block chain in an embodiment of the present invention;

FIG. 6 is a flowchart of implementation of step S20 in a KYC-based anti-money-laundering method by means of a block chain in an embodiment of the present invention;

FIG. 7 is a block diagram of a principle of a KYC-based anti-money-laundering apparatus by means of a block chain in an embodiment of the present invention; and

FIG. 8 is a schematic diagram of a computer device in an embodiment of the present invention.

Detailed Description of the Invention

The following further describes the present invention in detail with reference to the accompanying drawings.

A KYC-based anti-money-laundering method by means of a block chain provided by this application may be applied to the application environment shown in FIG. 1. A client (computer device) communicates with a server through a network. The client obtains user transaction information from the server and sends the user transaction information to the server. According to the user transaction information, the server retrieves the user transaction information from the third-party database and verifies the user transaction information. The client (computer device) may be, but is not limited to, various personal computers, notebook computers, smartphones, tablet computers, and portable wearable devices. The server may be implemented by a separate server or a server cluster composed of multiple servers.

Embodiment 1:

FIG. 2 shows a KYC-based anti-money-laundering method by means of a block chain disclosed in the present invention. That the method is applied to the server in FIG. 1 is used as an example for description, and the method includes the following steps.

S10: Obtain user identity information, and store the user identity information into a third-party database by using a block chain.

In this embodiment, the user identity information refers to information for recording user attributes, wherein the user identity information may include a name, an ID number, and a personal credit record of the user. The third-party database refers to a database for storing user identity information. The block chain refers to a novel application mode of computer technologies such as distributed data storage, point-to-point transmission, a consensus mechanism, and an encryption algorithm.

Specifically, the user identity information may be obtained from the user credit information system, and the user identity information is processed by using the block chain technology, and is

then stored into the third-party database.

S20: If user transaction information is obtained, obtain the user identity information from the third-party database.

In this embodiment, user transaction information refers to information triggered by a user to request a transaction. The user transaction information includes a user identity and specific transaction content for distinguishing each user.

Specifically, according to the user identity, the user identity information of the user is obtained in the third-party database.

S30: Verify the user identity information, and if verification succeeds, respond to the user transaction information

Specifically, the user identity information is verified, the identity information of the user and/or the credit record of the user are verified, and whether there is the risk of illegal behaviors such as money laundering is checked. If verification on the user identity information succeeds, then in response to the user transaction information, the user is allowed to perform transaction according to specific transaction content in the transaction information.

In this embodiment, user information is stored into the third-party database by using a block chain technology, so that user identification information can be retrieved during financial transaction without separate costs, and identity identification is performed on the user. In addition, by using the block chain technology, the decentralization of the block chain technology, and the cryptography technology in the block chain technology are used, so that the user identity information cannot be tampered and falsified, and can only be updated, so as to ensure the authenticity of the user identity information, thereby providing technical support for combating money laundering.

In an embodiment, as shown in FIG. 3, in step S10, namely, the user identity information is obtained, and the user identity information is stored into the third-party database by using the block chain, the following steps are specifically included.

S11: User identity information includes a user identity and a user historical transaction record.

In this embodiment, the user identity is an identifier for distinguishing each user. The user historical transaction record refers to information recording historical transactions of the user.

S12: Encrypt the user historical transaction record by using an asymmetric cryptographic algorithm, and store the encrypted user historical transaction record into a third-party database.

In this embodiment, the asymmetric cryptographic algorithm refers to a key encryption method. Specifically, after the user historical transaction record is encrypted by using the asymmetric cryptographic algorithm, the encrypted user historical transaction record and the user identity are stored into the third-party database.

In an embodiment, as shown in FIG. 4, in step S12, namely, the user historical transaction record is encrypted by using the asymmetric cryptographic algorithm and is stored into the third-party database, the following steps are specifically included.

S121: Each user historical transaction record includes corresponding transaction time and transaction content.

In this embodiment, at least one transaction record exists in the user historical transaction record. Each transaction record includes corresponding transaction time and transaction content.

S122: Calculate each historical transaction record by using a Hash algorithm, to obtain a corresponding block and Hash value.

In this embodiment, the Hash algorithm refers to converting input of any length (or referred to as a pre-image) into output of a fixed length by using a Hash algorithm, and the output is a Hash value. Specifically, each historical transaction record is sequentially calculated by using the Hash algorithm, to obtain a block and Hash value corresponding to each historical transaction record.

S123: Form a block corresponding to each historical transaction record into a block chain according to a sequence of transaction time.

Specifically, each historical transaction record calculated by using the Hash algorithm is formed into a corresponding block chain by using a block chain technology according to a sequence of the transaction time.

S124: Encrypt the block chain by using an asymmetric cryptographic algorithm, and store the block chain into a third-party database according to a user identity.

Specifically, the block chain is encrypted by using the asymmetric cryptographic algorithm, and is marked by using a user identity of a corresponding user, and is stored into the third-party database.

In an embodiment, as shown in FIG. 5, in step S124, namely, the block corresponding to each historical transaction record is formed into the block chain according to the sequence of the transaction time, the following steps are specifically included.

S1241: Calculate a first historical transaction record by using a Hash algorithm according to a sequence of transaction time, to obtain a first block and a first Hash value.

In this embodiment, the first historical transaction record of the user is selected according to the sequence of the transaction time, and the first historical transaction record is calculated by using the Hash algorithm to obtain the first Hash value, and the transaction time of the first historical transaction record and the first has value are used as a first block.

Specifically, the transaction content in the first historical transaction record is used as input of the Hash algorithm, and by means of calculation by using a hash function, the first Hash value is obtained.

S1242: Calculate an Mth historical transaction record and an (M-1)th Hash value starting from a

second historical transaction record by using the Hash algorithm, to obtain an Mth block and an Mth Hash value, and form the first, second, ..., Mth blocks into a block chain, wherein M is a positive integer greater than or equal to 2.

In this embodiment, starting from the second historical transaction record, the first Hash value corresponding to the first historical transaction record and the second historical transaction record are used as input of the Hash algorithm, to obtain a second Hash value by means of calculation, and the transaction time of the first historical transaction record and the second Hash value are used as a second block, until the Mth historical transaction record obtains the Mth block and the Mth Hash value by using the Hash algorithm.

Further, the blocks are connected in a chain manner to obtain the block chain in a manner of corresponding each block to a Hash value of a previous block according to the sequence of the transaction time.

In an embodiment, as shown in FIG. 6, in step S20, namely, the block corresponding to each historical transaction record is formed into the block chain according to the sequence of the transaction time, the following steps are specifically included.

S21: An asymmetric cryptographic algorithm includes a public key and a private key.

In this embodiment, the public key refers to a key that encrypts the block chain in the asymmetric cryptographic algorithm. The private key refers to a key for decryption when information in the block chain is viewed. The public key is different from the private key, and therefore the encryption algorithm is referred to as an asymmetric cryptographic algorithm.

S22: Encrypt a block chain by using the public key, and store the encrypted block chain into a third-party database.

Specifically, after user historical transaction information in the block chain is encrypted by using the public key, the encrypted information is transmitted and stored into the third-party database.

S23: User transaction information includes a user identity, and obtain, from the third-party database according to the user identity, a corresponding block chain after encryption.

Specifically, according to the user identity in the user transaction information, the block chain corresponding to the user is obtained from the third-party database.

S24: Decrypt, by using the private key, the corresponding block chain after encryption, to obtain user identity information.

Specifically, the private key is used for decryption, to obtain historical transaction information of the user.

Embodiment 2:

In an embodiment, a KYC-based anti-money-laundering apparatus by means of a block chain is provided. The KYC-based anti-money-laundering apparatus by means of a block chain is

one-to-one corresponding to the KYC-based anti-money-laundering method by means of a block chain in the foregoing embodiment. As shown in FIG. 7, the KYC-based anti-money-laundering apparatus by means of a block chain includes a first obtaining module 10, a second obtaining module 20, and a verification module 30. The functional modules are specifically described as follows:

The first obtaining module 10 is configured to: obtain user identity information, and store the user identity information into a third-party database by using a block chain.

The second obtaining module 20 is configured to: if user transaction information is obtained, obtain the user identity information from the third-party database.

The verification module 30 is configured to: verify the user identity information, and if verification succeeds, respond to the user transaction information.

Preferably, the first obtaining module 10 includes:

a user information submodule 11, for user identity information to include a user identity and a user historical transaction record; and

an encryption submodule 12, configured to encrypt the user historical transaction record by using an asymmetric cryptographic algorithm, and store the encrypted user historical transaction record into a third-party database.

Preferably, the encryption submodule 12 includes:

a transaction record unit 121, for allowing each user historical transaction record to include corresponding transaction time and transaction content;

a calculation unit 122, configured to calculate each historical transaction record by using a Hash algorithm, to obtain a corresponding block and Hash value;

a block chain forming unit 123, configured to form a block corresponding to each historical transaction record into a block chain according to a sequence of transaction time; and

a storage unit 124, configured to encrypt the block chain by using an asymmetric cryptographic algorithm, and store the block chain into a third-party database according to a user identity.

Preferably, the storage unit 124 includes:

a first calculation subunit 1241, configured to calculate a first historical transaction record by using a Hash algorithm according to a sequence of transaction time, to obtain a first block and a first Hash value; and

a second calculation subunit 1242, configured to calculate an Mth historical transaction record and an (M-1)th Hash value starting from a second historical transaction record by using the Hash algorithm, to obtain an Mth block and an Mth Hash value, and form the first, second, ..., Mth blocks into a block chain, wherein M is a positive integer greater than or equal to 2.

Preferably, the second obtaining module 20 includes:

a key submodule 21, for an asymmetric cryptographic algorithm to include a public key and a private key;

a public key encryption submodule 22, configured to: encrypt a block chain by using the public key, and store the encrypted block chain into a third-party database;

an obtaining submodule 23, for the user transaction information to include a user identity, and configured to obtain, from a third-party database according to the user identity, a corresponding block chain after encryption;

a private key decryption submodule 24, configured to decrypt, by using the private key, the corresponding block chain after encryption, to obtain user identity information.

For the specific limitation of the KYC-based anti-money-laundering apparatus by means of a block chain, reference may be made to the limitation of the KYC-based anti-money-laundering method by means of a block chain in the foregoing text, and details are not described herein again. Each module in the KYC-based anti-money-laundering apparatus by means of a block chain can be implemented in whole or in part by software, hardware, and a combination thereof. Each of the above modules may be embedded in or independent of the processor in the computer device in a hardware form, or may be stored in a memory in the computer device in a software form, so that the processor invokes the operations corresponding to the above modules.

Embodiment 3:

In an embodiment, a computer device is provided, which may be a server, and its internal structure diagram may be shown in FIG. 8. The computer device includes a processor, a memory, a network interface, and a database that are connected by using a system bus. The processor of the computer device is configured to provide computing and control capabilities. The memory of the computer device includes a non-volatile storage medium, an internal memory. The non-volatile storage medium stores an operating system, a computer program, and a database. The internal memory provides an environment for operation of the operating system and computer program in the non-volatile storage medium. The database of the computer device is configured to store user identity information. The network interface of the computer device is configured to communicate with an external terminal via a network connection. The computer program is executed by the processor to implement a KYC-based anti-money-laundering method by means of a block chain.

In an embodiment, a computer device is provided and includes a memory, a processor, and a computer program stored on the memory and operable on the processor, and when the processor executes the computer program, the following steps are implemented:

obtaining user identity information, and storing the user identity information into a third-party database by using a block chain;

if user transaction information is obtained, obtaining the user identity information from the

third-party database; and

verifying the user identity information, and if verification succeeds, responding to the user transaction information.

Embodiment 4:

In an embodiment, a computer readable storage medium storing a computer program is provided, and the following steps are implemented when the computer program is executed by a processor: obtaining user identity information, and storing the user identity information into a third-party database by using a block chain;

if user transaction information is obtained, obtaining the user identity information from the third-party database; and

verifying the user identity information, and if verification succeeds, responding to the user transaction information.

A person of ordinary skill in the art may understand that all or some of the processes of the methods in the foregoing embodiments may be implemented by a computer program instructing relevant hardware. The computer program may be stored in a non-volatile computer readable storage medium, and may include, for example, processes of the embodiments of the foregoing methods when executed. Any reference to a memory, storage, a database or another medium used in the embodiments provided in this application may include a non-volatile and/or volatile memory. The non-volatile memory may include a read-only memory (ROM), a programmable ROM (PROM), an electrically programmable ROM (EPROM), an electrically erasable programmable ROM (EEPROM), or a flash memory. The volatile memory may include a random access memory (RAM) or an external cache. By way of illustration instead of limitation, a RAM is available in a variety of forms, such as a static RAM (SRAM), a dynamic RAM (DRAM), a synchronous DRAM (SDRAM), a dual data rate SDRAM (DDRSDRAM), an enhanced SDRAM (ESDRAM), a synchronization link (Synchlink), a DRAM (SLDRAM), a memory Bus (Rambus) direct RAM (RDRAM), a direct memory bus dynamic RAM (DRDRAM), and a memory bus dynamic RAM (RDRAM).

A person skilled in the art can clearly learn that, for convenience and brevity of description, only the division of the foregoing functional units and modules is exemplified. In actual application, the foregoing functions may be assigned to different functional units and modules according to needs for completion. That is, the internal structure of the apparatus is divided into different functional units or modules to complete all or some of the functions described above.

The embodiments described above are only for explaining the technical solutions of the present invention, and are not intended to limit the technical solutions. Although the present invention has been described in detail with reference to the foregoing embodiments, a person of ordinary skill in

the art should understand that the technical solutions disclosed in the foregoing embodiments may still be modified or some of the technical features may be equivalently replaced. The modifications or replacements do not make the essence of corresponding technical solutions to depart from the spirit and scope of the technical solutions of the embodiments of the present invention, and should all fall within the protection scope of the present invention.

The embodiments of this specific implementation are all preferred embodiments of the present invention, and are not intended to limit the protection scope of the present invention. Therefore, any equivalent change made according to the structures, shapes, and principles of the present invention should fall within the protection scope of the present invention.

Claims

1. A KYC-based anti-money-laundering method comprising:
 - obtaining a user identity information, and storing the user identity information into a third-party database by using a block chain;
 - if a user transaction information is obtained, obtaining the user identity information from the third-party database according to the user transaction information;
 - verifying the user identity information obtained from the third-party database, and
 - if verification succeeds, responding to the user transaction information.
2. The KYC-based anti-money-laundering method according to claim 1, wherein the step of obtaining a user identity information, and storing the user identity information into a third-party database by using a block chain comprises:
 - the user identity information comprising a user identity and a user historical transaction record; and
 - encrypting the user historical transaction record by using an asymmetric cryptographic algorithm, and
 - storing the encrypted user historical transaction record into the third-party database.
3. The KYC-based anti-money-laundering method according to claim 2, wherein the steps of encrypting the user historical transaction record by using an asymmetric cryptographic algorithm, and storing the encrypted user historical transaction record into the third-party database comprise:
 - each user historical transaction record comprising corresponding transaction time and transaction content;
 - calculating each historical transaction record by using a Hash algorithm, to obtain a corresponding block and Hash value;
 - forming the block corresponding to each historical transaction record into a block chain according to a sequence of the transaction time; and
 - encrypting the block chain by using the asymmetric cryptographic algorithm, and
 - storing the block chain into the third-party database according to the user identity.
4. The KYC-based anti-money-laundering method according to claim 3, wherein the step of forming the block corresponding to each historical transaction record into a block chain according to a sequence of the transaction time comprises:
 - calculating a first historical transaction record by using the Hash algorithm according to the sequence of the transaction time, to obtain a first block and a first Hash value; and
 - calculating an Mth historical transaction record and an (M-1)th Hash value starting from a second historical transaction record by using the Hash algorithm, to obtain an Mth block and an Mth Hash value, and
 - forming the first, second, ..., Mth blocks into the block chain, wherein M is a positive integer greater than or equal to 2.
5. The KYC-based anti-money-laundering method according to claim 3, wherein the step of if a

user transaction information is obtained, obtaining the user identity information from the third-party database according to the user transaction information comprises:

the asymmetric cryptographic algorithm comprising a public key and a private key;

encrypting the block chain by using the public key, and storing the encrypted block chain into the third-party database;

the user transaction information comprising the user identity, and obtaining, from the third-party database according to the user identity, the corresponding block chain after encryption; and

decrypting, by using the private key, the corresponding block chain after encryption, to obtain the user identity information.

6. A KYC-based anti-money-laundering apparatus comprising:

a first obtaining module, configured to: obtain a user identity information, and store the user identity information into a third-party database by using a block chain;

a second obtaining module, configured to: if a user transaction information is obtained, obtain the user identity information from the third-party database according to the user transaction information; and

a verification module, configured to: verify the user identity information obtained from the third-party database, and if verification succeeds, respond to the user transaction information.

7. The KYC-based anti-money-laundering apparatus according to claim 6, wherein the first obtaining module further comprises:

a user information submodule, for allowing the user identity information to comprise a user identity and a user historical transaction record; and

an encryption submodule, configured to: encrypt the user historical transaction record by using an asymmetric cryptographic algorithm, and store the encrypted user historical transaction record into the third-party database.

8. The KYC-based anti-money-laundering apparatus according to claim 7, wherein the encryption submodule comprises:

a transaction record unit, for allowing each user historical transaction record to comprise corresponding transaction time and transaction content;

a calculation unit, configured to calculate each historical transaction record by using a Hash algorithm, to obtain a corresponding block and Hash value;

a block chain forming unit, configured to form the block corresponding to each historical transaction record into a block chain according to a sequence of the transaction time; and

a storage unit, configured to: encrypt the block chain by using the asymmetric cryptographic algorithm, and store the block chain into the third-party database according to the user identity.

9. A computer device, comprising a memory, a processor, and a computer program that is stored in the memory and that can run on the processor, wherein when the processor executes the computer program, the steps of the KYC-based anti-money-laundering method according to any one of claims 1 to 5 are implemented.

10. A computer readable storage medium, storing a computer program, wherein when the computer program is executed by a processor, the steps of the KYC-based anti-money-laundering method according to any one of claims 1 to 5 are implemented.