

DIGITAL CERTIFICATE PROCESSING METHOD AND RELATED APPARATUS

The present application claims priority to the Chinese Patent Application No. 201811175201.X, filed with the Chinese Patent Office on October 9, 2018 and entitled "DIGITAL CERTIFICATE PROCESSING METHOD AND RELATED APPARATUS", which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

The present application relates to the field of blockchain technologies, and in particular, to a digital certificate processing method and a related apparatus.

BACKGROUND

At present, many consortium blockchain applications begin to introduce a digital certificate authority (Certificate Authority, CA) to issue a digital certificate to a participant on a blockchain. Because many participants (for example, most banks) have their own CAs, they expect to issue digital certificates to customers by using their own CAs. For example, bank A, bank B, and bank C all have their own CAs, which are CA-A, CA-B, and CA-C, respectively. All of the banks can issue digital certificates to respective customers by using their own CAs. In a consortium blockchain network, any participant such as bank A, bank B, or bank C accepts a digital certificate issued to its customer by a CA of another participant. However, all participants on a consortium blockchain can determine, based on a digital certificate of a customer, a participant to which the customer belongs. For example, bank B can determine, based on an issuer of a digital certificate of an enterprise, a bank whose customers include the enterprise. For example, if the digital certificate of the enterprise is issued by bank A, bank B can determine that the enterprise is a customer of bank A. At present, issuing a digital certificate on a consortium blockchain causes information about a consortium blockchain transaction to be completely open to all participants on the consortium blockchain, and identities of both transaction parties be inevitably exposed. Therefore, it is difficult to satisfy transaction requirements of all participants, and applicability is poor.

SUMMARY

Embodiments of the present application provide a digital certificate processing method and a related apparatus, which can anonymously issue a digital certificate and enhance identity privacy of a digital certificate issuer, and have strong applicability.

According to a first aspect, an embodiment of the present application provides a digital certificate issuing method, where the method is applicable to a digital certificate issuer, and the method includes:

recording, by a certificate authority CA of a first participant in a blockchain network, a CA public key of the first participant in the blockchain network, where the first participant is a digital certificate issuer in the blockchain network, a CA public key of at least one second participant is further recorded in the blockchain network, and the second participant is a participant other than the first participant in the blockchain network;

when receiving a certificate authorization request of any user, confirming, by the CA of the first participant based on user identity information carried in the certificate authorization request, whether the user is a user of the CA of the first participant;

if confirming that the user is a user of the CA of the first participant, obtaining, by the CA of the first participant, a public key of the user from the certificate authorization request, and obtaining CA public keys of any N second participants from the blockchain network based on a preset ring signature certificate issuing rule, where N is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

performing, by the CA of the first participant, ring signature on the user identity information and the public key of the user based on the public key and a private key of the CA of the first participant and the CA public keys of the N second participants and forming a digital certificate; and sending the digital certificate to the user.

According to a second aspect, an embodiment of the present application provides a digital certificate verification method, where the method is applicable to a digital certificate verifier, and the method includes:

obtaining, by the verifier, a digital certificate of an initiator of any signature transaction in a blockchain network when the verifier obtains the signature transaction, where the initiator of the signature transaction can be one of participants in the blockchain network, and certificate authority CA public keys of all the participants including the initiator of the transaction are

recorded in the blockchain network;

obtaining, by the verifier, public key information of a ring signature of the digital certificate from the digital certificate based on a preset ring signature certificate issuing rule, and determining all public keys corresponding to the ring signature of the digital certificate based on the public key information, where all the public keys corresponding to the ring signature are CA public keys of a plurality of participants in the blockchain network, and a quantity of public keys corresponding to the ring signature is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

verifying, by the verifier, a signature of the signature transaction based on all the public keys corresponding to the ring signature.

According to a third aspect, an embodiment of the present application provides a digital certificate issuing apparatus, where the apparatus is applicable to a certificate authority CA of a digital certificate issuer, and the apparatus includes:

a recording unit, configured to record a CA public key of a first participant in a blockchain network, where the first participant is a digital certificate issuer in the blockchain network, a CA public key of at least one second participant is further recorded in the blockchain network, and the second participant is a participant other than the first participant in the blockchain network;

a confirmation unit, configured to: when a certificate authorization request of any user is received, confirm, based on user identity information carried in the certificate authorization request, whether the user is a user of a CA of the first participant;

an obtaining unit, configured to: when the confirmation unit confirms that the user is a user of the CA of the first participant, obtain a public key of the user from the certificate authorization request, and obtain CA public keys of any N second participants from the blockchain network based on a preset ring signature certificate issuing rule, where N is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

an issuing unit, configured to perform ring signature on the user identity information and the public key of the user based on the public key and a private key of the CA of the first participant and the CA public keys of the N second participants and form a digital certificate; and send the digital certificate to the user.

According to a fourth aspect, an embodiment of the present application provides a digital certificate verification apparatus, where the apparatus is applicable to a digital certificate verifier,

and the apparatus includes:

an obtaining unit, configured to obtain a digital certificate of an initiator of any signature transaction in a blockchain network when obtaining the signature transaction, where the initiator of the signature transaction can be one of participants in the blockchain network, and certificate authority CA public keys of all the participants including the initiator of the transaction are recorded in the blockchain network;

a determining unit, configured to obtain public key information of a ring signature of the digital certificate from the digital certificate based on a preset ring signature certificate issuing rule, and determine all public keys corresponding to the ring signature of the digital certificate based on the public key information, where all the public keys corresponding to the ring signature are CA public keys of a plurality of participants in the blockchain network, and a quantity of public keys corresponding to the ring signature is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

a verification unit, configured to verify a signature of the signature transaction based on all the public keys corresponding to the ring signature that are determined by the determining unit.

According to a fifth aspect, an embodiment of the present application provides a terminal, where the terminal includes a processor, a memory, and a transceiver, or a processor and a memory; the processor, the memory, and the transceiver, or the processor and the memory are connected to each other; the memory is configured to store a computer program; the computer program includes program instructions; and the processor and the transceiver are or the processor is configured to invoke the program instructions to execute the method provided in the first aspect or the method provided in the second aspect.

According to a sixth aspect, an embodiment of the present application provides a computer-readable storage medium, where the computer-readable storage medium stores a computer program, the computer program includes program instructions, and when the program instructions are being executed by a processor, the processor is enabled to execute the method provided in the first aspect or the method provided in the second aspect.

Based on the embodiments of the present application, unconditional anonymity of any participant serving as a digital certificate authority can be implemented, the digital certificate authority can anonymously issue digital certificates to its users, an identity of the digital certificate authority can be prevented from being disclosed, and other participants in the

blockchain network can be prevented from knowing information about the digital certificate authority, thereby enhancing identity privacy of the digital certificate authority, and ensuring privacy of transaction information of the digital certificate authority. The embodiments of the present application have strong applicability.

BRIEF DESCRIPTION OF DRAWINGS

To describe the technical solutions of the embodiments of the present application more clearly, the following briefly describes the accompanying drawings required for describing the embodiments.

FIG. 1 is a schematic diagram of a general digital certificate issuing process according to an embodiment of the present application;

FIG. 2 is a schematic flowchart of a digital certificate processing method according to an embodiment of the present application;

FIG. 3 is a schematic structural diagram of a digital certificate issuing apparatus according to an embodiment of the present application;

FIG. 4 is a schematic structural diagram of a digital certificate verification apparatus according to an embodiment of the present application;

FIG. 5 is a schematic structural diagram of a terminal according to an embodiment of the present application; and

FIG. 6 is another schematic structural diagram of a terminal according to an embodiment of the present application.

DETAILED DESCRIPTION

The following clearly and completely describes the technical solutions in the embodiments of the present application with reference to the accompanying drawings in the embodiments of the present application.

A digital certificate processing method provided in the embodiments of the present application (which includes a digital certificate issuing method and a digital certificate verification method, and for convenience of description, is hereinafter referred to as a method

provided in the embodiments of the present application) and a related apparatus are applicable to application scenarios such as service transaction and/or enterprise information processing of institutions such as banks, insurance companies, security companies, business associations, group enterprises, and upstream and downstream enterprises. Details may be specifically determined based on an actual application scenario, and are not limited herein. Optionally, the preceding institutions may serve as a plurality of participants in one consortium blockchain network. Optionally, the preceding institutions may have respective consortium blockchain networks. In the respective consortium blockchain networks of the preceding institutions, customers and/or staff of the institutions may be participants in the consortium blockchain networks. Details may be specifically determined based on an actual application scenario, and are not limited herein. For convenience of description, the following provides descriptions by using an example in which the institutions may serve as a plurality of participants in one consortium blockchain network. For convenience of understanding, the following briefly describes a consortium blockchain and a digital certificate involved in the method provided in the embodiments of the present application.

I. Consortium blockchain

The blockchain is born in the era of mobile Internet. The institutions such as banks, insurance companies, security companies, business associations, group enterprises, and upstream and downstream enterprises have generally become IT-based and Internet-based organizations and/or institutions. The blockchain is very helpful in further improving processing efficiency of services such as notarization, settlement and clearing, and value exchange in industrial chains of these institutional circles. However, processing performance, privacy protection, compliance, and the like of conventional blockchains (such as public blockchains) cannot meet service requirements of these institutions. If public blockchains are used to process the services such as notarization, settlement and clearing, and value exchange, existing business models and inherent interests of these institutions are subverted, and risks are high. Therefore, based on the service requirements of the institutions, a blockchain system with better privacy protection, namely, the consortium blockchain, emerges. The consortium blockchain is specific only to members of a specific group and a limited quantity of third parties, and inside the consortium blockchain, a plurality of preselected nodes are designated as bookkeepers. Generation of each block is jointly determined by all the preselected nodes, and other access nodes can participate in a transaction, but do not make inquiry about an accounting process. Other third parties can perform limited query by using an open application programming interface (Application Programming Interface, API) of the consortium blockchain. With the admission mechanism, performance and privacy of a

transaction between participants in a consortium blockchain network can be enhanced.

II. Digital certificate

The digital certificate is a string of digits used to identify identity information of each communicator in Internet communications. Emergence of the digital certificate provides the Internet communications with a manner of verifying a communications entity identity of each communicator on the Internet. A digital certificate is not a digital identity card, but a seal or a stamp on a digital identity card of each communications entity (or a signature added to the digital identity card of each communications entity) by an identity authentication authority of the communications entity. The digital certificate is issued by an authoritative institution, namely, a CA, and the digital certificate can be used on the Internet to identify an identity of each communications entity. The digital certificate is a file digitally signed by the CA, where the file contains holder information of a public key and a file of the public key. A simplest digital certificate can contain a public key, a holder name of the public key, and a digital signature of a certificate authority, and the digital certificate is valid only for a specific period of time.

The digital certificate is an authoritative electronic document, and may be issued by an authoritative and impartial third-party institution, namely, a CA (for example, a Chinese local CA company) or may be issued by an enterprise-class CA (for example, CA-A of bank A). The digital certificate can be used for secure electronic affairs processing and secure electronic transaction signature, such as secure email sending, secure website access, online securities transactions, online tendering and purchasing, online office, online insurance, online taxation, online contract signing, and online banking. The digital certificate stores many digits and English letters. When the digital certificate is used for identity authentication, the digital certificate randomly generates a 128-digit identity code. Each digital certificate can generate a corresponding different digital code each time to ensure confidentiality of data transmission, which is equivalent to generating a complex password. The digital certificate binds a public key and a real identity of a holder of the public key. The digital certificate is similar to a resident identity card in the real life. A difference lies in that the digital certificate is no longer a paper certificate, but a piece of electronic data that contains identity information of a holder of the digital certificate and that is approved and issued by a certificate authority. Therefore, the digital certificate can be more conveniently and flexibly used in e-commerce and e-government affairs.

FIG. 1 is a schematic diagram of a general digital certificate issuing process according to an embodiment of the present application. The digital certificate issuing process provided in this

embodiment of the present application generally includes the following steps S11 and S12:

S11. A user sends a certificate authorization request to a CA of an institution.

In some feasible implementations, when the user (for example, a customer of an institution such as a bank, an insurance company, or an enterprise) requests a transaction with the institution (for example, a bank, an insurance company, or an enterprise), the user may first generate its own key pair, where the key pair includes a public key and a private key, and transmit the public key and some user identity information to the CA of the institution by sending the certificate authorization request to the CA of the institution. In other words, the certificate authorization request sent by the user to the CA of the institution may include some user identity information and the public key of the user, to request the CA of the institution to sign the user identity information and the public key of the user and issue a digital certificate.

S12. The CA of the institution verifies an identity of the user and issues a digital certificate.

In some feasible implementations, the institution with which the user requests the signature transaction may verify the identity of the user by using the CA of the institution. When the CA of the institution verifies the identity of the user (that is, verifies that the user is its own customer), the CA of the institution may determine the user identity information included in the certificate authorization request sent by the user, to confirm that the certificate authorization request is actually sent by its own customer (namely, the user). When confirming that the certificate authorization request is sent by the user, the CA of the institution sends a digital certificate to the user. The digital certificate contains the user identity information and the public key of the user, as well as signature information of the CA of the institution. Therefore, the user can sign the related transaction by using the digital certificate issued by the CA of the institution. A digital certificate issued by a CA of each institution to its customer is issued by an independent certificate authority (namely, CA) of the institution. Digital certificates vary, each type of certificate can provide a different level of credibility, and each customer (namely, user) of each institution can obtain its own digital certificate from a CA of the institution.

The digital certificate uses a public key system, that is, uses a pair of keys that match each other, for digital signature and signature verification. Each user self-sets a specific private key known only by the user, and can digitally sign information about a transaction with an institution based on the private key. Meanwhile, the user can set a corresponding public key, and the public key is made public by the user and shared by a group of users, and is used to verify a signature of the transaction information. The public key technology resolves a key release

management problem, and the user can make the public key hold by the user public and keep the private key hold by the user. The user can also use its own private key to process the transaction information. In this way, because the private key is owned by only the user, a file that other persons cannot generate is generated, that is, a digital signature is formed. Use of the digital signature can ensure that transaction information is self-signed and sent by a transmitter, and therefore the transmitter cannot deny or is difficult to deny the transaction information, and can also ensure that no modification is made to the transaction information from a moment at which the transmitter signs the transaction information to a moment at which a receiver receives the transaction information, and therefore the issued document is a real document, thereby ensuring tamper-resistance of the transaction information.

Based on the characteristic of the consortium blockchain and the characteristic of the digital certificate, the embodiments of the present application provide a digital certificate processing method based on a distributed digital certificate and a related apparatus, including a digital certificate issuing method and apparatus and a digital certificate verification method and apparatus, which can issue a digital certificate to a customer of any participant in a consortium blockchain network, and can determine, based on a digital certificate of an initiator of any signature transaction, all public keys corresponding to a ring signature of the digital certificate, to verify a signature of the transaction based on all the public keys corresponding to the ring signature of the digital certificate. A CA of each participant in a consortium blockchain can issue a digital certificate to its own customer based on the digital certificate issuing method provided in the embodiments of the present application, to implement unconditional anonymity of a CA of any participant serving as a signer (namely, a digital certificate issuer), thereby preventing an identity of the CA of the digital certificate issuer from being disclosed, and preventing the other participants in the consortium blockchain network from knowing customer information of the CA of the digital certificate issuer. Therefore, privacy of transaction information of the digital certificate issuer and security of the customer information of the issuer can be ensured, and the method has stronger applicability. For details, refer to the implementations provided in the following embodiments. Specifically, in the method provided in the embodiments of the present application, public keys of CAs of all recognizable participants (for example, CA-A of bank A and CA-B of bank B) (or non-participants) in a consortium blockchain network can be recorded by using the consortium blockchain network. When a CA of any institution needs to issue a digital certificate to its own customer (or user), the CA of the institution issues the digital certificate to the customer by using a ring signature (conventionally, the CA uses its own private

key to sign the digital certificate issued by the CA to its customer). In this way, a third party cannot determine an institution whose CA issues the digital certificate. In other words, the third party cannot determine a recognized participant in the consortium blockchain network, where the customer is a customer of a CA of the recognized participant. Therefore, a CA of each recognized participant can anonymously send a digital certificate, thereby protecting privacy when a digital certificate is issued by the CA of each recognized participant in the consortium blockchain network to its customer, improving identity privacy of the CA of the digital certificate issuer, and enhancing applicability of the data certificate issuing manner.

FIG. 2 is a schematic flowchart of a digital certificate processing method according to an embodiment of the present application. Referring to FIG. 2, for an implementation in which a CA of any participant included in a consortium blockchain network uses a ring signature to issue a digital certificate to its own customer and any verifier performs signature verification on any signature transaction, refer to the implementation provided in the following steps S21 to S25. For convenience of description, the following provides descriptions by using an implementation in which a CA of any participant issues a digital certificate to its own customer (or user) as example, where the any participant may be described by using an issuer (namely, a first participant) as an example. In other words, the issuer herein is any participant in the consortium blockchain network that needs to issue a digital certificate to its own user. Correspondingly, any institution that verifies a digital certificate may be described by using a verifier as an example. Details may be specifically determined based on an actual application scenario, and are not limited herein.

S21. A CA of an issuer records its own public key in a blockchain network.

In some feasible implementations, a CA (or referred to as a participant CA) of any recognized participant (hereinafter referred to as a participant for convenience of description) in the consortium blockchain network (namely, the blockchain network) generates a public key and a private key, and can record information about the CA of the recognized participant (namely, the participant CA) and the public key in the consortium blockchain network by using a smart crypto contract (Smart Crypto Contract, SCC). For example, for many recognized banks, a CA of each bank can generate a public key and a private key, the public key generated by the CA of each bank can be made public by the CA of the bank itself and the public key of the CA of each bank is recorded in the consortium blockchain network, and the private key of the CA of each bank is known by the CA of the bank itself. In other words, assuming that the issuer is one of participants in the consortium blockchain network (assuming that the issuer is a first participant), in addition to the public key of the CA (or referred to as the CA public key) of the issuer (for convenience of

description, the digital certificate issuer in the blockchain network may be described by using the first participant as an example), CA public keys of participants other than the issuer (for convenience of description, any participant other than the digital certificate issuer in the blockchain network may be described by using a second participant as an example) are further recorded in the consortium blockchain network.

It may be understood that, CA public keys of all participants are recorded in the consortium blockchain network, and therefore any participant in the consortium blockchain can know CA public keys of all other participants in the consortium blockchain network. When a CA of any participant (for example, the first participant, namely, the issuer) needs to sign a digital certificate of its own customer (which is a customer of the CA of the issuer, and also is a customer of the issuer; for convenience of description, the following provides descriptions by using the customer of the CA of the issuer as an example), the CA of the participant can use a ring signature to obtain CA public keys of one or more other participants from the consortium blockchain network, and issue the digital certificate to its own customer in combination with its own public key and private key (namely, the public key and a private key of the CA of the issuer). For details, refer to the following step descriptions.

S22. When receiving a certificate authorization request of any user, the CA of the issuer confirms, based on user identity information carried in the certificate authorization request, whether the user is its own user.

In some feasible implementations, when any user (for example, any customer of bank A) requests a transaction with an institution (such as bank A), the user can deliver a public key and user identity information to the CA of the issuer (for convenience of description, for example, the CA of the issuer is a CA of bank A) by sending a certificate authorization request (or referred to as authentication request) to the CA of bank A. In other words, the certificate authorization request sent by the user to the CA of the issuer may include the user identity information and the public key of the user, to request the CA of the issuer to sign the user identity information and the public key of the user and issue a digital certificate to the user. The CA of the issuer can verify an identity of the user (that is, verify whether the user is its own customer) based on the user identity information included in the certificate authorization request, that is, the CA of the issuer can determine the user identity information included in the certificate authorization request sent by the user, to confirm that the certificate authorization request is actually sent by its own customer. After determining that the user sending the certificate authorization request is its own user (namely, a user of the CA of the issuer, namely, a user of a CA of the first participant), the CA of

the issuer can issue a digital certificate to the user.

S23. If confirming that the user is its own user, the CA of the issuer obtains a public key of the user from the certificate authorization request, and obtains CA public keys of any other N participants from the blockchain network based on a preset ring signature certificate issuing rule.

In some feasible implementations, a ring signature certificate issuing rule (that is, a rule of issuing a digital certificate by using a ring signature) of each participant may be self-formulated by a CA of the participant, and the CA of each participant can randomly select one or more third-party public keys (for convenience of description, assuming that the CA of each participant can randomly select N third-party public keys) based on its own requirement, and complete ring signature in combination with its own public key and private key. For a CA of any participant in any consortium blockchain network, the N third-party public keys randomly selected by the CA can be CA public keys recorded in the consortium blockchain network by CAs of any N participants other than the participant. In other words, in a ring signature certificate issuing rule self-formulated by any participant, a quantity of public keys used by a CA of the participant to issue a digital certificate to its user may be self-set by the CA of the participant. Optionally, CAs of all participants in the consortium blockchain network may jointly formulate a ring signature certificate issuing rule and write the ring signature certificate issuing rule into the consortium blockchain network, where the ring signature certificate issuing rule includes but is not limited to a quantity of public keys required for a ring signature and specifications, and may be set in advance within the consortium blockchain network. No limitation is imposed herein.

Optionally, in some feasible implementations, a ring signature certificate issuing rule self-formulated by each participant may be written into the consortium blockchain network, where the ring signature certificate issuing rule includes but is not limited to a quantity of public keys required for a ring signature and specifications (namely, specifications composed of a digital certificate in an X509 format, such as a digital certificate format (X509) and/or a preset field used to record public key information of a ring signature in X509), and may be set in advance within the consortium blockchain network. For example, a quantity of public keys required when a CA of each participant (for example, a CA of each issuer) in the consortium blockchain network uses a ring signature to issue a digital certificate to its own user, the specifications composed of the digital certificate in the X509 format (or referred to as ring signature certificate issuing specifications), and the like may be set in advance within the consortium blockchain network, thereby helping a verifier verify a signature of a transaction in the consortium blockchain network based on information such as the specifications. The preset field used to record the public key

information of the ring signature in X509 includes but is not limited to an issuer label field and/or an extension field in the digital certificate format. Details may be specifically determined based on an actual application scenario and are not limited herein.

Optionally, X509 includes an extension (Extension) field, and the extension field may be used to record all public keys corresponding to a ring signature of a digital certificate (for example, CA public keys of N participants corresponding to the ring signature), and/or public key information such as identifiers of all the public keys corresponding to the ring signature (for example, the CA public keys of the N participants corresponding to the ring signature). The verifier determines all public keys corresponding to the ring signature based on all the public keys recorded in the extension field included in X509, and/or searches the consortium blockchain network for the corresponding public keys based on the identifiers of the all the public keys recorded in the extension field included in X509, to verify the signature of the transaction based on all the public keys corresponding to the ring signature.

Optionally, in some feasible implementations, in the consortium blockchain network, CA public keys of all participants in the consortium blockchain network may be divided into different public key groups, and a group identifier may be specified for each public key group. The group identifier of each group may help a verifier find a public key group (for convenience of description, a target group may be used as an example for description) corresponding to a ring signature, and then the verifier can determine public keys in the public key group corresponding to the ring signature as public keys corresponding to the ring signature, so that the verifier can obtain information about CAs to which the public keys belong. The verifier determines the public key information of the ring signature based on the extension field in X509, where the public key information of the ring signature includes a group identifier, and then the verifier can determine the target group from the plurality of public key groups recorded in the consortium blockchain network based on the group identifier included in the digital certificate, so that the verifier can determine all the public keys included in the target group as all the public keys corresponding to the ring signature, to verify the signature of the transaction based on all the public keys corresponding to the ring signature.

S24. The CA of the issuer performs ring signature on the user identity information and a public key of the user based on the public key and a private key of the CA of the issuer and CA public keys of any other N participants and forms a digital certificate; and sends the digital certificate to the user.

N is equal to a public key quantity that is set in the preset ring signature certificate issuing rule in step S23.

In some feasible implementations, when a CA of any participant (namely, issuer, for example, bank A) in the consortium blockchain network prepares to issue a digital certificate to its own customer (namely, user, for example, enterprise 1), the CA of the issuer uses its own public key and private key (for example, a public key and a private key of a CA of bank A) and CA public keys of any other participants (for example, CA public keys of other banks, where it is assumed that N public keys are used, and it may be understood that the CA public keys of the plurality of participants are recorded in the consortium blockchain network) in the consortium blockchain network to sign identity information and a public key of enterprise 1 and form a digital certificate, and public key information of a ring signature of the digital certificate is carried in a preset field in X509 of the digital certificate. For example, it is assumed that the CA of bank A receives a certificate authorization request of its customer (assuming that the customer is m), where the certificate authorization request includes some user identity information and the user's public key that needs to be verified. In this case, after the CA of bank A verifies an identity of the user corresponding to the user identity information carried in the certificate authorization request and confirms that m is actually its own customer, the CA of bank A can use CA public keys of N ring members in the consortium blockchain and the public key and the private key of the CA of bank A as input, to apply for generating a signature R for the public key and the identity information of customer m. The CA of bank A can issue a digital certificate (the certificate includes basic information and the public key of the customer) signed with R to the customer, and therefore the customer can sign a transaction by using the digital certificate issued by the CA of bank A to the customer.

In some feasible implementations, the CA of the issuer in the consortium blockchain network uses a conventional X509 format to issue a digital certificate to its own customer, and the issued digital certificate complies with the ITU-TX.509 international standard. It should be noted that, X509 is used to issue a digital certificate, but a label of the certificate issuer (Issuer) in X509 is no longer a name of an institution, but a blockchain network (for example, a consortium blockchain network) identifier corresponding to the CA of the certificate issuer. It is assumed that the label of the certificate issuer in X509 is a field in X509, and the blockchain network identifier corresponding to the CA of the certificate issuer is recorded in the field. For convenience of description, it is assumed that the field is an issuer label field. In other words, the issuer label field in X509 may be any field used to record the blockchain network identifier corresponding to

the CA of the certificate issuer in X509. Details may be specifically determined based on an actual application scenario, and are not limited herein.

Optionally, public key indication information corresponding to the CA of the certificate issuer (Issuer) is recorded in the label of the certificate issuer in X509. The public key indication information includes but is not limited to all public key information corresponding to the ring signature of the digital certificate and the identifiers of all the public keys corresponding to the ring signature of the digital certificate. In other words, the public key indication information corresponding to the CA of the certificate issuer may be recorded in the issuer label field in X509, and the public key indication information includes but is not limited to all the public key information corresponding to the ring signature of the digital certificate and the identifiers of all the public keys corresponding to the ring signature of the digital certificate. No limitation is imposed herein.

Optionally, the public key information corresponding to the CA of the issuer may be recorded in an extension (Extension) field in X509. The public key information includes but is not limited to all the public keys corresponding to the ring signature of the digital certificate and the identifiers of all the public keys corresponding to the ring signature of the digital certificate. Optionally, the public key group identifier corresponding to the ring signature of the digital certificate may be recorded in the extension field in X509, where the public key group identifier is used to indicate the group to which the public keys corresponding to the ring signature of the digital certificate belong, to help the digital certificate verifier find the public keys corresponding to the ring signature based on the group to which the public keys belong.

Optionally, in some feasible implementations, if a ring signature certificate issuing rule is formulated based on specifications (for example, centrally formulated or agreed on) in the consortium blockchain network, the extension field in X509 does not need to record more information. Details may be specifically determined based on an actual application scenario, and are not limited herein.

S25. When a verifier obtains any signature transaction in the blockchain network, the verifier obtains a digital certificate of an initiator of the transaction, obtains public key information of a ring signature from the digital certificate based on a preset ring signature certificate signing rule, determines all public keys corresponding to the ring signature based on the public key information, and verifies a signature of the transaction based on all the public keys corresponding to the ring signature.

In some feasible implementations, the verifier may be any institution, and is not limited herein. The following provides descriptions by using any participant in the consortium blockchain network as an example, and no specific limitation is imposed herein. The ring signature certificate issuing rule is recorded in the blockchain network. The ring signature certificate issuing rule includes a quantity of public keys of the ring signature and ring signature certificate issuing specifications. The ring signature certificate issuing specifications include a preset field used to record the public key information of the ring signature in the digital certificate format X509. The public key information included in the digital certificate includes a blockchain network identifier included in the preset field in the digital certificate format X509, and CA public keys of all participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of all the participants corresponding to the ring signature of the digital certificate. The preset field includes an issuer label field and/or an extension field. Optionally, if CA public keys of all participants recorded in the consortium blockchain network are divided into a plurality of groups and one group corresponds to one group identifier, the public key information may include a group identifier included in the digital certificate, where the group identifier is used to determine a target group included in the blockchain network, to determine the CA public keys of all the participants corresponding to the ring signature of the digital certificate based on public keys included in the target group. For details, refer to the verifier operation manner corresponding to the signature of the digital certificate in step S24. No limitation is imposed herein.

In some feasible implementations, when any signature transaction is received in the consortium blockchain network, the verifier in the consortium blockchain network can obtain a digital certificate of an initiator of the signature transaction upon obtaining the signature transaction. The data certificate format is X509, and the verifier can find all public keys corresponding to a ring signature of the digital certificate of the initiator from the consortium blockchain network based on an identifier written into X509. In other words, when verifying a signature of any signature transaction, the verifier can find all public keys corresponding to a ring signature of a digital certificate from the consortium blockchain network based on an identifier written into X509 when an initiator of the transaction issues the digital certificate. Optionally, the verifier may find, based on a digital certificate of a transaction initiator, public key information written into an issuer (Issuer) label in X509 (for example, public key information included in an issuer label field in X509), where the public key information includes but is not limited to all public keys corresponding to a ring signature of the digital certificate and/or identifiers of all the

public keys corresponding to the ring signature of the digital certificate. Optionally, the verifier may find, based on a digital certificate of a transaction initiator, public key information written into an extension field in X509, where the public key information includes but is not limited to all public keys corresponding to a ring signature of the digital certificate and/or identifiers of all the public keys corresponding to the ring signature of the digital certificate. Optionally, the verifier may find, based on a digital certificate of a transaction initiator, a public key group identifier written into an extension field in X509, and find, based on the public key group identifier, a group to which public keys corresponding to a ring signature of the digital certificate belong from the public key groups included in the consortium blockchain network, and then may determine all the public keys corresponding to the ring signature of the digital certificate based on the found group to which the public keys belong. In specific implementation, a manner based on which the verifier finds the public keys corresponding to the ring signature may be specifically determined based on information in X509, and is not limited herein. After finding all the public keys corresponding to the ring signature of the digital certificate of the transaction initiator, the verifier can verify the signature of the transaction based on all the found public keys. A specific verification process is not limited herein. In other words, specific information, in the digital certificate, that carries and/or indicates the public key information of the ring signature of the digital certificate is not limited herein. In other words, a specific field, in the digital certificate format (X509), that carries and/or indicates the public key information of the ring signature of the digital certificate is not limited herein. For details, refer to the verifier operation manner corresponding to the signature of the digital certificate in step S24. No limitation is imposed herein.

It can be learned from the foregoing description that, implementing ring signature on a digital certificate based on the method provided in this embodiment of the present application can implement unconditional anonymity of an issuer of the digital certificate. The issuer is exactly anonymous to a verifier. The implementing ring signature on a digital certificate based on the method provided in this embodiment of the present application includes but is not limited to the following security attributes:

(1) Unconditional anonymity. Even if an attacker illegally obtains private keys of all possible signers, a probability that the attacker can determine a true signer does not exceed $1/n$, where n is a quantity of ring members (namely, possible signers).

(2) Non-forgery. Without knowing a private key of any ring member, even if an attacker can obtain a signature of any user from a random predictor that generates a ring signature, a

probability that the attacker can successfully forge a valid signature of the user can almost be ignored.

(3) The ring signature has a good characteristic. The ring signature can implement unconditional anonymity of a signer, and the signer can freely specify its own anonymity range, so that a main function of a group signature can be implemented without a trusted third party, a group administrator, or the like.

In this embodiment of the present application, issuing a digital certificate to a user of a CA of an issuer based on a ring signature certificate issuing rule self-formulated by the CA of the digital certificate issuer can ensure that a CA of any participant other than the CA of the issuer of the digital certificate cannot determine a participant whose CA issues the digital certificate. In other words, a CA of any participant other than the CA of the issuer of the digital certificate in the consortium blockchain network cannot determine a participant in the consortium blockchain, where a receiver of the digital certificate is a customer of a CA of the participant. Therefore, privacy can be implemented when a digital certificate is issued by a CA of each participant in the consortium blockchain to its user, the CA of each participant can anonymously send the digital certificate to its user, identity privacy of the CA of the issuer of the digital certificate can be ensured, information security of a transaction between the CA of each participant in the consortium blockchain network and its user can be enhanced, more business requirements of participants in the consortium blockchain network can be met, and the method has stronger applicability.

FIG. 3 is a schematic structural diagram of a digital certificate issuing apparatus according to an embodiment of the present application. The digital certificate issuing apparatus is applicable to a digital certificate issuer. The digital certificate issuer may be any participant that needs to issue a digital certificate to its own user in a consortium blockchain network, and is not limited herein. The digital certificate issuing apparatus may include:

a recording unit 31, configured to record a CA public key of a first participant in a blockchain network, where the first participant is a digital certificate issuer in the blockchain network, a CA public key of at least one second participant is further recorded in the blockchain network, and the second participant is a participant other than the first participant in the blockchain network;

a confirmation unit 32, configured to: when a certificate authorization request of any user is received, confirm, based on user identity information carried in the certificate authorization

request, whether the user is a user of a CA of the first participant;

an obtaining unit 33, configured to: when the confirmation unit 32 confirms that the user is a user of the CA of the first participant, obtain a public key of the user from the certificate authorization request, and obtain CA public keys of any other N second participants from the blockchain network based on a preset ring signature certificate issuing rule, where N is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

an issuing unit 34, configured to perform ring signature on the user identity information and the public key of the user based on the public key and a private key of the CA of the first participant and the CA public keys of the N second participants and form a digital certificate; and send the digital certificate to the user.

In some feasible implementations, the ring signature certificate issuing rule is self-formulated by the CA of the first participant or jointly formulated by CAs of all participants in the blockchain network; and the ring signature certificate issuing rule is recorded in the blockchain network.

In some feasible implementations, the ring signature certificate issuing rule further includes specifications composed of a digital certificate in X509, and X509 includes a preset field used to record public key information of a ring signature; and

the issuing unit 34 is configured to:

perform ring signature on the user identity information and the public key of the user based on the specifications by using the public key and the private key of the CA of the first participant and the CA public keys of the N second participants and form the digital certificate, where a preset field of the digital certificate carries public key information of a ring signature of the digital certificate.

In some feasible implementations, X509 includes an issuer label field, and the issuer label field includes a blockchain network identifier corresponding to the CA of the first participant, and/or the public key information of the ring signature of the digital certificate; and

the public key information includes the CA public keys of the N second participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of the N second participants corresponding to the ring signature.

In some feasible implementations, the preset field includes an extension field in X509, and

the public key information that is of the ring signature and that is carried in the extension filed includes the CA public keys of the N second participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of the N second participants corresponding to the ring signature.

In some feasible implementations, CA public keys of all the participants recorded in the blockchain network are divided into a plurality of groups, and one group corresponds to one group identifier; and

the preset field includes an extension field in X509, the public key information that is of the ring signature and that is carried in the extension filed includes a group identifier, and the group identifier is used to indicate a group to which the CA public keys of the N second participants corresponding to the ring signature belong, to help a verifier of the digital certificate find the CA public keys of the N second participants based on the group to which the CA public keys of the N second participants belong.

In specific implementation, the digital certificate issuing apparatus serving as a digital certificate issuer can execute the implementations provided in the steps in the foregoing embodiment by using the function units built in the digital certificate issuing apparatus. Optionally, the recording unit 31 is configured to execute the implementation provided in step S21 in the foregoing embodiment. For details, refer to the operation performed by the digital certificate issuing apparatus in step S21. No limitation is imposed herein. The confirmation unit 32 is configured to perform the implementation provided in step S22 in the foregoing embodiment. For details, refer to the operation performed by the digital certificate issuing apparatus in step S22. No limitation is imposed herein. The obtaining unit 33 is configured to perform the implementation provided in step S23 in the foregoing embodiment. For details, refer to the operation performed by the digital certificate issuing apparatus in step S23. No limitation is imposed herein. The issuing unit 34 is configured to execute the implementation provided in step S24 in the foregoing embodiment. For details, refer to the operation performed by the digital certificate issuing apparatus in step S24. No limitation is imposed herein.

In this embodiment of the present application, the CA of the digital certificate issuer may self-formulate the ring signature certificate issuing rule, including a quantity of public keys required for a ring signature, ring signature certificate issuing specifications, and the like. Issuing a digital certificate to a user of the CA of the issuer based on the ring signature certificate issuing rule self-formulated by the CA of the digital certificate issuer can ensure that a CA of any

participant other than the CA of the digital certificate issuer cannot determine a participant whose CA issues the digital certificate. In other words, a CA of any participant other than the CA of the digital certificate issuer in the consortium blockchain network cannot determine a participant in the consortium blockchain, where a receiver of the digital certificate is a customer of a CA of the participant. Therefore, privacy can be implemented when a digital certificate is issued by a CA of each participant in the consortium blockchain to its user, the CA of each participant can anonymously send the digital certificate to its user, identity privacy of the CA of the issuer of the digital certificate can be ensured, information security of a transaction between the CA of each participant in the consortium blockchain network and its user can be ensured, more business requirements of participants in the consortium blockchain network can be met, and the apparatus has stronger applicability.

FIG. 4 is a schematic structural diagram of a digital certificate verification apparatus according to an embodiment of the present application. The digital certificate verification apparatus is applicable to a digital certificate verifier, and is not limited herein. The digital certificate verification apparatus may include:

an obtaining unit 41, configured to obtain a digital certificate of an initiator of any signature transaction in a blockchain network when obtaining the signature transaction, where the initiator of the signature transaction can be one of participants in the blockchain network, and certificate authority CA public keys of all the participants including the initiator of the transaction are recorded in the blockchain network;

a determining unit 42, configured to obtain public key information of a ring signature of the digital certificate from the digital certificate based on a preset ring signature certificate issuing rule, and determine all public keys corresponding to the ring signature of the digital certificate based on the public key information, where all the public keys corresponding to the ring signature are CA public keys of a plurality of participants in the blockchain network, and a quantity of public keys corresponding to the ring signature is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

a verification unit 43, configured to verify a signature of the signature transaction based on all the public keys corresponding to the ring signature that are determined by the determining unit 42.

In some feasible implementations, the ring signature certificate issuing rule is recorded in the blockchain network, the ring signature certificate issuing rule further includes specifications

composed of a digital certificate in X509, and X509 includes a preset field used to record public key information of a ring signature;

the public key information includes a blockchain network identifier included in the preset field, and/or CA public keys of all participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of all the participants; and

The preset field includes an issuer label field and/or an extension field.

In some feasible implementations, the ring signature certificate issuing rule is recorded in the blockchain network, the ring signature certificate issuing rule further includes specifications composed of a digital certificate in X509, and X509 includes a preset field used to record public key information of a ring signature;

the CA public keys of all the participants recorded in the blockchain network are divided into a plurality of groups, and one group corresponds to one group identifier; and

the public key information includes a group identifier included in the preset field, and the group identifier is used to determine a target group included in the blockchain network, to determine CA public keys of all participants corresponding to the ring signature of the digital certificate based on CA public keys included in the target group.

In specific implementation, the digital certificate verification apparatus serving as a verifier can execute, by using the function units built in the digital certificate verification apparatus, the implementations executed by the verifier in the foregoing embodiments, including but not limited to the operation performed by the verifier in the implementation provided in step S25. For details, refer to the implementations provided in the foregoing steps. Details are not described herein again.

In this embodiment of the present application, the verifier can determine the quantity of public keys required for the ring signature and the ring signature certificate issuing specifications based on the ring signature certificate issuing rule formulated by all the participants in the consortium blockchain network, and can determine all the public keys corresponding to the ring signature of the digital certificate based on the CA public keys of all the participants recorded in the consortium blockchain network. A transaction initiated by a digital certificate holder can be easily verified based on all public keys corresponding to a ring signature. Therefore, privacy of a CA identity of a digital certificate issuer is enhanced while the verification on the transaction is completed, service requirements of more participants can be met, and the apparatus has stronger

applicability.

FIG. 5 is a schematic structural diagram of a terminal according to an embodiment of the present application. The terminal is applicable to a digital certificate issuer. The issuer may be any participant that needs to issue a digital certificate to its own user in a consortium blockchain network. Details may be specifically determined based on an actual application scenario, and are not limited herein.

As shown in FIG. 5, the terminal in this embodiment may include one or more processors 501, a memory 502, and one or more transceivers 503. The processor 501, the memory 502, and the transceiver 503 are connected by using a bus 504. The memory 502 is configured to store a computer program, where the computer program includes program instructions. The processor 501 and the transceiver 503 are configured to execute the program instructions stored in the memory 502. The processor 501 and the transceiver 503 are configured to invoke the program instructions to perform the following operations:

The transceiver 503 is configured to send a CA public key of a first participant to a blockchain network and record the CA public key of the first participant in the blockchain network, where the first participant is a digital certificate issuer in the blockchain network, a CA public key of at least one second participant is further recorded in the blockchain network, and the second participant is a participant other than the first participant in the blockchain network.

The processor 501 is configured to: when the transceiver 503 receives a certificate authorization request of any user, confirm, based on user identity information carried in the certificate authorization request, whether the user is a user of a CA of the first participant; if confirming that the user is a user of the CA of the first participant, obtain a public key of the user from the certificate authorization request, and obtain CA public keys of any N second participants from the blockchain network based on a preset ring signature certificate issuing rule, where N is equal to a public key quantity that is set in the ring signature certificate issuing rule.

The processor 501 is further configured to perform ring signature on the user identity information and the public key of the user based on the public key and a private key of the CA of the first participant and the CA public keys of the N second participants and form a digital certificate.

The transceiver 503 is further configured to send the digital certificate to the user.

In some feasible implementations, the ring signature certificate issuing rule is

self-formulated by the CA of the first participant or jointly formulated by CAs of all participants in the blockchain network; and the ring signature certificate issuing rule is recorded in the blockchain network.

In some feasible implementations, the ring signature certificate issuing rule further includes specifications composed of a digital certificate in X509, and X509 includes a preset field used to record public key information of a ring signature; and

the processor 501 is configured to:

perform ring signature on the user identity information and the public key of the user based on the specifications by using the public key and the private key of the CA of the first participant and the CA public keys of the N second participants and form the digital certificate, where a preset field of the digital certificate carries public key information of a ring signature of the digital certificate.

In some feasible implementations, X509 includes an issuer label field, and the issuer label field includes a blockchain network identifier corresponding to the CA of the first participant, and/or the public key information of the ring signature of the digital certificate; and

the public key information includes the CA public keys of the N second participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of the N second participants corresponding to the ring signature.

In some feasible implementations, the preset field includes an extension field in X509, and the public key information that is of the ring signature and that is carried in the extension field includes the CA public keys of the N second participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of the N second participants corresponding to the ring signature.

In some feasible implementations, CA public keys of all the participants recorded in the blockchain network are divided into a plurality of groups, and one group corresponds to one group identifier; and

the preset field includes an extension field in X509, the public key information that is of the ring signature and that is carried in the extension field includes a group identifier, and the group identifier is used to indicate a group to which the CA public keys of the N second participants corresponding to the ring signature belong, to help a verifier of the digital certificate find the CA public keys of the N second participants based on the group to which the CA public keys of the N

second participants belong.

In some feasible implementations, the processor 501 may be a central processing unit (central processing unit, CPU). Alternatively, the processor may be another general-purpose processor, a digital signal processor (digital signal processor, DSP), an application-specific integrated circuit (application-specific integrated circuit, ASIC), a field-programmable gate array (field-programmable gate array, FPGA) or another programmable logic device, a discrete gate or transistor logic device, a discrete hardware component, or the like. The general-purpose processor may be a microprocessor, or may be any conventional processor or the like.

The memory 502 may include a read-only memory and a random access memory, and provides instructions and data for the processor 501 and the transceiver 503. A part of the memory 502 may further include a nonvolatile random access memory. For example, the memory 502 may further store device type information.

In some feasible implementations, the terminal may perform the operations by using the function modules built in the terminal, such as the processor 501 and the transceiver 503, as performed by the CA of the issuer in the implementations provided in the steps in the foregoing embodiments. For details, refer to the implementations provided in the steps. Details are not described herein again.

In this embodiment of the present application, the terminal serving as a CA of a digital certificate issuer may self-formulate the ring signature certificate issuing rule, including a quantity of public keys required for a ring signature, ring signature certificate issuing specifications, and the like. Issuing a digital certificate to a user of the CA of the issuer based on the ring signature certificate issuing rule self-formulated by the CA of the digital certificate issuer can ensure that a CA of any participant other than the CA of the digital certificate issuer cannot determine a participant whose CA issues the digital certificate. In other words, a CA of any participant other than the CA of the digital certificate issuer in the consortium blockchain network cannot determine a participant in the consortium blockchain, where a receiver of the digital certificate is a customer of a CA of the participant. Therefore, privacy can be implemented when a digital certificate is issued by a CA of each participant in the consortium blockchain to its user, the CA of each participant can anonymously send the digital certificate to its user, identity privacy of the CA of the issuer of the digital certificate can be ensured, information security of a transaction between the CA of each participant in the consortium blockchain network and its user can be ensured, more business requirements of participants in the consortium blockchain network

can be met, and the apparatus has stronger applicability.

FIG. 6 is another schematic structural diagram of a terminal according to an embodiment of the present application. The terminal is applicable to a digital certificate verifier. As shown in FIG. 6, the terminal in this embodiment may include one or more processors 601 and a memory 602. The processor 601 and the memory 602 are connected by using a bus 603. The memory 602 is configured to store a computer program, where the computer program includes program instructions. The processor 601 is configured to execute the program instructions stored in the memory 602. The processor 601 is configured to invoke the program instructions to perform the following operations:

obtaining, by the verifier, a digital certificate of an initiator of any signature transaction in a blockchain network when obtaining the signature transaction, where the initiator of the signature transaction can be one of participants in the blockchain network, and certificate authority CA public keys of all the participants including the initiator of the transaction are recorded in the blockchain network;

obtaining public key information of a ring signature of the digital certificate from the digital certificate based on a preset ring signature certificate issuing rule, and determining all public keys corresponding to the ring signature of the digital certificate based on the public key information, where all the public keys corresponding to the ring signature are CA public keys of a plurality of participants in the blockchain network, and a participant quantity of the plurality of participants is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

verifying a signature of the signature transaction based on all the public keys corresponding to the ring signature.

In some feasible implementations, the ring signature certificate issuing rule is recorded in the blockchain network, the ring signature certificate issuing rule further includes specifications composed of a digital certificate in X509, and X509 includes a preset field used to record public key information of a ring signature;

the public key information includes a blockchain network identifier included in the preset field, and/or CA public keys of all participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of all the participants; and

The preset field includes an issuer label field and/or an extension field.

In some feasible implementations, the ring signature certificate issuing rule is recorded in

the blockchain network, the ring signature certificate issuing rule further includes specifications composed of a digital certificate in X509, and X509 includes a preset field used to record public key information of a ring signature;

the CA public keys of all the participants recorded in the blockchain network are divided into a plurality of groups, and one group corresponds to one group identifier; and

the public key information includes a group identifier included in the preset field, and the group identifier is used to determine a target group included in the blockchain network, to determine CA public keys of all participants corresponding to the ring signature of the digital certificate based on CA public keys included in the target group.

In some feasible implementations, the terminal may perform the operations by using the function components built in the terminal, such as the processor 601, as performed by the verifier in the implementations provided in the steps in the foregoing embodiments. For details, refer to the implementations provided in the steps. Details are not described herein again.

In this embodiment of the present application, the terminal serving as a digital certificate verifier can determine the quantity of public keys required for the ring signature and the ring signature certificate issuing specifications based on the ring signature certificate issuing rule formulated by the CAs of all the participants in the consortium blockchain network, and can determine all the public keys corresponding to the ring signature of the digital certificate based on the CA public keys of all the participants recorded in the consortium blockchain network. A transaction initiated by a digital certificate holder can be easily verified based on all public keys corresponding to a ring signature. Therefore, privacy of a CA identity of a digital certificate issuer is enhanced while the verification on the transaction is completed, service requirements of more participants can be met, and the terminal has stronger applicability.

An embodiment of the present application further provides a computer-readable storage medium. The computer-readable storage medium stores a computer program, the computer program includes program instructions, and when the program instructions are being executed by a processor, the method provided in the steps in FIG. 2 is implemented. For details, refer to the implementations provided in the steps. Details are not described herein again.

The computer-readable storage medium may be the digital certificate issuing apparatus provided in any of the foregoing embodiments or an internal storage unit of the foregoing terminal, such as a hard disk or a memory of an electronic device. Alternatively, the

computer-readable storage medium may be an external storage device of the electronic device, such as a plug-in hard disk, a smart media card (smart media card, SMC), a secure digital (secure digital, SD) card, or a flash card (flash card) equipped on the electronic device. Further, the computer-readable storage medium may include both the internal storage unit and the external storage device of the electronic device. The computer-readable storage medium is configured to store the computer program and other programs and data required by the electronic device. The computer-readable storage medium may be further configured to temporarily store data that has been or is to be output.

The terms "include" and "have" and any variations thereof in the claims, specification, and accompanying drawings of the present application are intended to cover non-exclusive inclusion. "Embodiment" herein means that a specific feature, structure or characteristic described in combination with an embodiment may be included in at least one embodiment of the present application. Presenting the phrase at various locations in this specification does not necessarily mean same embodiments, or separate or alternative embodiments mutually exclusive with other embodiments. The term "and/or" used in this specification and appended claims of the present application means one or any combination of a plurality of associated listed items and all possible combinations, and means that these combinations are included.

CLAIMS

What is claimed is:

1. A digital certificate issuing method, wherein the method is applicable to a digital certificate issuer, and the method comprises:

recording, by a certificate authority CA of a first participant in a blockchain network, a CA public key of the first participant in the blockchain network, wherein the first participant is a digital certificate issuer in the blockchain network, a CA public key of at least one second participant is further recorded in the blockchain network, and the second participant is a participant other than the first participant in the blockchain network;

when receiving a certificate authorization request of any user, confirming, by the CA of the first participant based on user identity information carried in the certificate authorization request, whether the user is a target user, wherein the target user is a user of the CA of the first participant;

if confirming that the user is a target user, obtaining, by the CA of the first participant, a public key of the user from the certificate authorization request, and obtaining CA public keys of any N second participants from the blockchain network based on a preset ring signature certificate issuing rule, wherein N is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

performing, by the CA of the first participant, ring signature on the user identity information and the public key of the user based on the public key and a private key of the CA of the first participant and the CA public keys of the N second participants and forming a digital certificate; and sending the digital certificate to the user.

2. The method according to claim 1, wherein the ring signature certificate issuing rule is self-formulated by the CA of the first participant or jointly formulated by CAs of all participants in the blockchain network; and the ring signature certificate issuing rule is recorded in the blockchain network.

3. The method according to claim 2, wherein the ring signature certificate issuing rule further comprises specifications composed of a digital certificate in X509, and X509 comprises a preset field used to record public key information of a ring signature; and

the performing, by the CA of the first participant, ring signature on the user identity information and the public key of the user based on the public key and a private key of the CA of

the first participant and the CA public keys of the N second participants and forming a digital certificate comprises:

performing, by the CA of the first participant, ring signature on the user identity information and the public key of the user based on the specifications by using the public key and the private key of the CA of the first participant and the CA public keys of the N second participants and forming the digital certificate, wherein a preset field of the digital certificate carries public key information of a ring signature of the digital certificate.

4. The method according to claim 3, wherein X509 comprises an issuer label field, and the issuer label field comprises a blockchain network identifier corresponding to the CA of the first participant, and/or the public key information of the ring signature of the digital certificate; and

the public key information comprises the CA public keys of the N second participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of the N second participants corresponding to the ring signature.

5. The method according to claim 3, wherein the preset field comprises an extension field in X509, and the public key information that is of the ring signature and that is carried in the extension field comprises the CA public keys of the N second participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of the N second participants corresponding to the ring signature.

6. The method according to claim 3, wherein CA public keys of all the participants recorded in the blockchain network are divided into a plurality of groups, and one group corresponds to one group identifier; and

the preset field comprises an extension field in X509, the public key information that is of the ring signature and that is carried in the extension field comprises a group identifier, and the group identifier is used to indicate a group to which the CA public keys of the N second participants corresponding to the ring signature belong, to help a verifier of the digital certificate find the CA public keys of the N second participants based on the group to which the CA public keys of the N second participants belong.

7. A digital certificate verification method, wherein the method is applicable to a digital certificate verifier and the method comprises:

obtaining, by the verifier, a digital certificate of an initiator of any signature transaction in a blockchain network when the verifier obtains the signature transaction;

obtaining, by the verifier, public key information of a ring signature of the digital certificate from the digital certificate based on a preset ring signature certificate issuing rule, and determining all public keys corresponding to the ring signature of the digital certificate based on the public key information, wherein all the public keys corresponding to the ring signature are CA public keys of a plurality of participants in the blockchain network, and a quantity of public keys corresponding to the ring signature is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

verifying, by the verifier, a signature of the signature transaction based on all the public keys corresponding to the ring signature.

8. The method according to claim 7, wherein the ring signature certificate issuing rule is recorded in the blockchain network, the ring signature certificate issuing rule further comprises specifications composed of a digital certificate in X509, and X509 comprises a preset field used to record public key information of a ring signature;

the public key information comprises a blockchain network identifier comprised in the preset field, and/or CA public keys of all participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of all the participants; and

the preset field comprises an issuer label field and/or an extension field.

9. The method according to claim 7, wherein the ring signature certificate issuing rule is recorded in the blockchain network, the ring signature certificate issuing rule further comprises specifications composed of a digital certificate in X509, and X509 comprises a preset field used to record public key information of a ring signature;

CA public keys of all participants recorded in the blockchain network are divided into a plurality of groups, and one group corresponds to one group identifier; and

the public key information comprises a group identifier comprised in the preset field, and the group identifier is used to determine a target group comprised in the blockchain network, to determine CA public keys of all participants corresponding to the ring signature of the digital certificate based on CA public keys comprised in the target group.

10. A digital certificate issuing apparatus, wherein the apparatus is applicable to a certificate authority CA of a digital certificate issuer, and the apparatus comprises:

a recording unit, configured to record a CA public key of a first participant in a blockchain

network, wherein the first participant is a digital certificate issuer in the blockchain network, a CA public key of at least one second participant is further recorded in the blockchain network, and the second participant is a participant other than the first participant in the blockchain network;

a confirmation unit, configured to: when a certificate authorization request of any user is received, confirm, based on user identity information carried in the certificate authorization request, whether the user is a user of a CA of the first participant;

an obtaining unit, configured to: when the confirmation unit confirms that the user is a user of the CA of the first participant, obtain a public key of the user from the certificate authorization request, and obtain CA public keys of any N second participants from the blockchain network based on a preset ring signature certificate issuing rule, wherein N is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

an issuing unit, configured to perform ring signature on the user identity information and the public key of the user based on the public key and a private key of the CA of the first participant and the CA public keys of the N second participants and form a digital certificate; and send the digital certificate to the user.

11. The apparatus according to claim 10, wherein the ring signature certificate issuing rule is self-formulated by the CA of the first participant or jointly formulated by CAs of all participants in the blockchain network; and the ring signature certificate issuing rule is recorded in the blockchain network.

12. The apparatus according to claim 11, wherein the ring signature certificate issuing rule further comprises specifications composed of a digital certificate in X509, and X509 comprises a preset field used to record public key information of a ring signature; and

the issuing unit is configured to:

perform ring signature on the user identity information and the public key of the user based on the specifications by using the public key and the private key of the CA of the first participant and the CA public keys of the N second participants and form the digital certificate, wherein a preset field of the digital certificate carries public key information of a ring signature of the digital certificate.

13. The apparatus according to claim 12, wherein X509 comprises an issuer label field, and the issuer label field comprises a blockchain network identifier corresponding to the CA of the

first participant, and/or the public key information of the ring signature of the digital certificate; and

the public key information comprises the CA public keys of the N second participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of the N second participants corresponding to the ring signature.

14. The apparatus according to claim 12, wherein the preset field comprises an extension field in X509, and the public key information that is of the ring signature and that is carried in the extension field comprises the CA public keys of the N second participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of the N second participants corresponding to the ring signature.

15. The apparatus according to claim 12, wherein CA public keys of all participants recorded in the blockchain network are divided into a plurality of groups, and one group corresponds to one group identifier; and

the preset field comprises an extension field in X509, the public key information that is of the ring signature and that is carried in the extension field comprises a group identifier, and the group identifier is used to indicate a group to which the CA public keys of the N second participants corresponding to the ring signature belong, to help a verifier of the digital certificate find the CA public keys of the N second participants based on the group to which the CA public keys of the N second participants belong.

16. A digital certificate verification apparatus, wherein the apparatus is applicable to a digital certificate verifier and the apparatus comprises:

an obtaining unit, configured to obtain a digital certificate of an initiator of any signature transaction in a blockchain network when obtaining the signature transaction;

a determining unit, configured to obtain public key information of a ring signature of the digital certificate from the digital certificate based on a preset ring signature certificate issuing rule, and determine all public keys corresponding to the ring signature of the digital certificate based on the public key information, wherein all the public keys corresponding to the ring signature are CA public keys of a plurality of participants in the blockchain network, and a quantity of public keys corresponding to the ring signature is equal to a public key quantity that is set in the ring signature certificate issuing rule; and

a verification unit, configured to verify a signature of the transaction based on all the public

keys corresponding to the ring signature that are determined by the determining unit.

17. The apparatus according to claim 16, wherein the ring signature certificate issuing rule is recorded in the blockchain network, the ring signature certificate issuing rule further comprises specifications composed of a digital certificate in X509, and X509 comprises a preset field used to record public key information of a ring signature;

the public key information comprises a blockchain network identifier comprised in the preset field, and/or CA public keys of all participants corresponding to the ring signature of the digital certificate, and/or identifiers of the CA public keys of all the participants; and

the preset field comprises an issuer label field and/or an extension field.

18. The apparatus according to claim 16, wherein the ring signature certificate issuing rule is recorded in the blockchain network, the ring signature certificate issuing rule further comprises specifications composed of a digital certificate in X509, and X509 comprises a preset field used to record public key information of a ring signature;

CA public keys of all the participants recorded in the blockchain network are divided into a plurality of groups, and one group corresponds to one group identifier; and

the public key information comprises a group identifier comprised in the preset field, and the group identifier is used to determine a target group comprised in the blockchain network, to determine CA public keys of all participants corresponding to the ring signature of the digital certificate based on CA public keys comprised in the target group.

19. A terminal, comprising a processor, a transceiver, and a memory, wherein the processor, the transceiver, and the memory are connected to each other, the memory is configured to store a computer program, the computer program comprises program instructions, and the processor and the transceiver are configured to invoke the program instructions to execute the method according to any one of claims 1 to 6 or the method according to any one of claims 7 to 9.

20. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program, the computer program comprises program instructions, and when the program instructions are being executed by a processor, the processor is enabled to execute the method according to any one of claims 1 to 6 or the method according to any one of claims 7 to 9.