

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property  
Organization  
International Bureau

(10) International Publication Number

WO 2019/023454 A1

(43) International Publication Date  
31 January 2019 (31.01.2019)(51) International Patent Classification:  
**H04L 29/06** (2006.01)      **H04L 9/32** (2006.01)  
**G06Q 20/38** (2012.01)      **H04L 29/08** (2006.01)  
**G06Q 20/40** (2012.01)(72) Inventor: **QIU, Honglin**; c/o Ants Patent Team, 17F Building B, Huanglong Times Plaza, No. 17 Wantang Road, Hangzhou, 310099 (CN).(74) Agent: **STALFORD, Terry, J.**; Fish & Richardson P.C., P.O. Box 1022, Minneapolis, MN 55440-1022 (US).(21) International Application Number:  
PCT/US2018/043901(22) International Filing Date:  
26 July 2018 (26.07.2018)(25) Filing Language:  
English(26) Publication Language:  
English(30) Priority Data:  
201710617611.4      26 July 2017 (26.07.2017)      CN(71) Applicant: **ALIBABA GROUP HOLDING LIMITED**  
[—/US]; Fourth Floor, One Capital Place, P.O. Box 847, George Town (KY).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,

(54) Title: DIGITAL CERTIFICATE MANAGEMENT METHOD AND APPARATUS, AND ELECTRONIC DEVICE

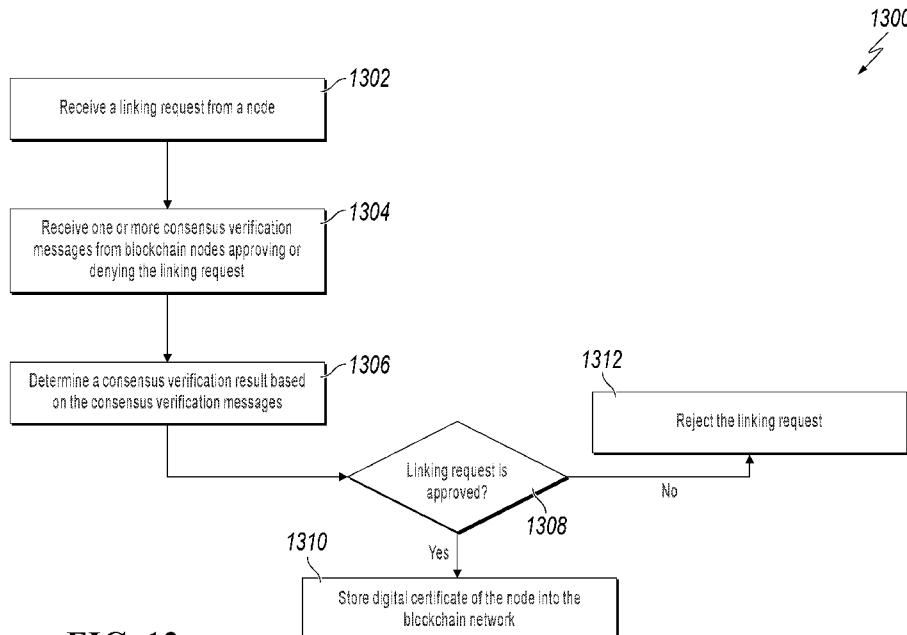


FIG. 13

(57) Abstract: A digital certificate linking request sent by a node in a blockchain is received, where the digital certificate linking request comprises a to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain. A consensus verification result of the to-be-verified digital certificate of the node is determined. A determination is performed, based on the consensus verification result, of whether to write the to-be-verified digital certificate into the blockchain.



UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Published:**

— *with international search report (Art. 21(3))*

## **DIGITAL CERTIFICATE MANAGEMENT METHOD AND APPARATUS, AND ELECTRONIC DEVICE**

### **CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] This application claims priority to Chinese Patent Application No. 5 201710617611.4, filed on July 26, 2017, which is hereby incorporated by reference in its entirety.

### **TECHNICAL FIELD**

[0002] The present application relates to the field of computer technologies, and in particular, to a digital certificate management method and apparatus, and an electronic 10 device.

### **BACKGROUND**

[0003] With the development of computer technologies, the blockchain technology (also referred to as the distributed ledger technology) has been favored for its decentralization, 15 openness and transparency, non-tampering, and trustiness, and is widely applied to many fields such as intelligent contracts, securities transactions, E-commerce, the Internet of Things, social communication, file storage, existence proofs, identity verification, and equity crowdsourcing.

[0004] Currently, a blockchain system can be mainly divided into three types: a public blockchain (Public Blockchain), a private blockchain (Private Blockchain), and a consortium 20 blockchain (Consortium Blockchain). The three types of blockchains mainly differ in openness objects. The public blockchain can be open to all individuals, the private blockchain is only open to an individual or entity organization, and the consortium blockchain is between the public blockchain and the private blockchain, open to a specific individual or entity organization, but not to other individual or entity organizations.

[0005] In a blockchain, especially in the consortium blockchain for a specific 25 organization, to improve communication security, a Certificate Authority (CA) center is usually designed to issue a node certificate to each node that participates in blockchain communication, so that only nodes having an authorized certificate can communicate with each other. In the existing technology, both the issued node certificate and information about 30 certificate validity such as a certificate revocation list are stored in a server of the CA center.

When nodes in the blockchain need to communicate with each other, information about the certificate validity stored in the CA center is called and queried, so as to confirm the certificate validity and complete communication process verification. The main drawbacks of this approach are:

5 [0006] Both the node digital certificate and the information about the certificate validity are stored in the CA center. Once the CA center is hacked, a hacker can arbitrarily modify the information about the certificate validity. For example, the hacker can tamper with the certificate revocation list to recover a revoked certificate back to normal. The hacker can further illegally join the blockchain by using a previously revoked problematic certificate, 10 and the node in the blockchain can confirm the certificate validity based on the tampered information, thereby threatening the security of the blockchain. Moreover, a private key of the CA center can also be hacked by the hacker, and the hacker can arbitrarily issue the digital certificate, threatening the security of a blockchain network.

## SUMMARY

15 [0007] Implementations of the present application provide a digital certificate management method, apparatus, and a corresponding electronic device, to improve the security of a blockchain network.

[0008] The following technical solutions are used in the implementations of the present application:

20 [0009] According to a first aspect, an implementation of the present application provides a digital certificate management method, including: receiving a digital certificate linking request sent by a node in a blockchain, where the digital certificate linking request includes a to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the 25 blockchain; determining a consensus verification result of the to-be-verified digital certificate of the node; and determining, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain.

[0010] Preferably, in the digital certificate management method provided in the first aspect, the determining a consensus verification result of the to-be-verified digital certificate of the node includes: determining verification results of nodes participating in consensus 30 verification in the blockchain; determining the number of first nodes and/or the number of

second nodes in the nodes participating in consensus verification, where a verification result of the first node is passing the consensus verification, and a verification result of the second node is not passing the consensus verification; and determining the consensus verification result based on the number of first nodes and/or the number of second nodes.

5 [0011] Preferably, in the digital certificate management method provided in the first aspect, the determining the consensus verification result based on the number of first nodes includes: when the number of first nodes satisfies a first predetermined condition, determining that the consensus verification result is passing the consensus verification; and the first predetermined condition includes one or more of the following: the number of first 10 nodes reaches a first predetermined threshold; a ratio of the number of first nodes to the number of nodes participating in consensus verification reaches a second predetermined threshold; and a ratio of the number of first nodes to the number of nodes in the blockchain reaches a third predetermined threshold.

15 [0012] Preferably, in the digital certificate management method provided in the first aspect, the determining, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain includes: writing the to-be-verified digital certificate into the blockchain when the consensus verification result is passing the consensus verification.

20 [0013] Preferably, in the digital certificate management method provided in the first aspect, the method further includes: receiving a digital certificate revocation request sent by the node in the blockchain, where the digital certificate revocation request includes a digital certificate of a target node that is requested to be revoked; determining a consensus verification result of the digital certificate of the target node; and determining, based on the consensus verification result, whether to revoke the digital certificate of the target node.

25 [0014] According to a second aspect, an implementation of the present application provides a digital certificate management method, including: receiving a digital certificate revocation request sent by a node in a blockchain, where the digital certificate revocation request includes a digital certificate of a target node that is requested to be revoked; determining a consensus verification result of the digital certificate of the target node; and determining, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain.

30 [0015] Preferably, in the digital certificate management method provided in the second

aspect, the determining a consensus verification result of the digital certificate of the target node includes: determining verification results of nodes participating in consensus verification in the blockchain; determining the number of first nodes and/or the number of second nodes in the nodes participating in consensus verification, where a verification result 5 of the first node is passing the consensus verification, and a verification result of the second node is not passing the consensus verification; and determining the consensus verification result based on the number of first nodes and/or the number of second nodes.

[0016] Preferably, in the digital certificate management method provided in the second aspect, the determining the consensus verification result based on the number of first nodes 10 includes: when the number of first nodes satisfies a first predetermined condition, determining that the consensus verification result is passing the consensus verification; and the first predetermined condition includes one or more of the following: the number of first nodes reaches a first predetermined threshold; a ratio of the number of first nodes to the number of nodes participating in consensus verification reaches a second predetermined 15 threshold; and a ratio of the number of first nodes to the number of nodes in the blockchain reaches a third predetermined threshold.

[0017] Preferably, in the digital certificate management method provided in the second aspect, the determining, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain includes: revoking the digital certificate 20 of the target node in the blockchain when the consensus verification result is passing the consensus verification.

[0018] According to a third aspect, an implementation of the present application provides a digital certificate management method, including: sending, by a node in a blockchain, a digital certificate linking request to the blockchain, so that the blockchain determines a 25 consensus verification result of a to-be-verified digital certificate of the node, and determines, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain, where the digital certificate linking request includes the to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the 30 blockchain.

[0019] According to a fourth aspect, an implementation of the present application provides a digital certificate management method, including: sending, by a node in a

blockchain, a digital certificate revocation request to the blockchain, so that the blockchain determines a consensus verification result of a digital certificate of a target node, and determines, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain, where the digital certificate revocation request 5 includes the digital certificate of the target node that is requested to be revoked.

[0020] According to a fifth aspect, an implementation of the present application provides a digital certificate management apparatus, where the apparatus is applied to a blockchain and includes: a request receiving module, configured to receive a digital certificate linking request sent by a node in the blockchain, where the digital certificate linking request includes 10 a to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain; a consensus verification result determining module, configured to determine a consensus verification result of the to-be-verified digital certificate of the node; and a certificate management module, configured to determine, based on the consensus verification 15 result, whether to write the to-be-verified digital certificate into the blockchain.

[0021] According to a sixth aspect, an implementation of the present application provides an electronic device, where the electronic device is applied to a blockchain and includes: a processor; and a storage, configured to store a computer executable instruction, where when the executable instruction is being executed, the processor performs the following operations: 20 receiving a digital certificate linking request sent by a node in the blockchain, where the digital certificate linking request includes a to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain; determining a consensus verification result of the to-be-verified digital certificate of the node; and determining, based on the 25 consensus verification result, whether to write the to-be-verified digital certificate into the blockchain.

[0022] According to a seventh aspect, an implementation of the present application provides a digital certificate management apparatus, where the apparatus is applied to a blockchain and includes: a request receiving module, configured to receive a digital certificate revocation request sent by a node in the blockchain, where the digital certificate revocation request includes a digital certificate of a target node that is requested to be revoked; 30 a consensus verification result determining module, configured to determine a consensus

verification result of the digital certificate of the target node; and a certificate management module, configured to determine, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain.

[0023] According to an eighth aspect, an implementation of the present application provides an electronic device, where the electronic device is applied to a blockchain and includes: a processor; and a storage, configured to store a computer executable instruction, where when the executable instruction is being executed, the processor performs the following operations: receiving a digital certificate revocation request sent by a node in the blockchain, where the digital certificate revocation request includes a digital certificate of a target node that is requested to be revoked; determining a consensus verification result of the digital certificate of the target node; and determining, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain.

[0024] According to a ninth aspect, an implementation of the present application provides a digital certificate management apparatus, where the apparatus is applied to a node in a blockchain and includes: a request initiation module, configured to send a digital certificate linking request to the blockchain, so that the blockchain determines a consensus verification result of a to-be-verified digital certificate of the node, and determines, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain, where the digital certificate linking request includes the to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain.

[0025] According to a tenth aspect, an implementation of the present application provides an electronic device, where the electronic device is applied to a node in a blockchain and includes: a processor; and a storage, configured to store a computer executable instruction, where when the executable instruction is being executed, the processor performs the following operation: sending a digital certificate linking request to the blockchain, so that the blockchain determines a consensus verification result of a to-be-verified digital certificate of the node, and determines, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain, where the digital certificate linking request includes the to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain.

[0026] According to an eleventh aspect, an implementation of the present application provides a digital certificate management apparatus, where the apparatus is applied to a node in a blockchain and includes: a request initiation module, configured to send a digital certificate revocation request to the blockchain, so that the blockchain determines a consensus verification result of a digital certificate of a target node, and determines, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain, where the digital certificate revocation request includes the digital certificate of the target node that is requested to be revoked.

[0027] According to a twelfth aspect, an implementation of the present application provides an electronic device, where the electronic device is applied to a node in a blockchain and includes: a processor; and a storage, configured to store a computer executable instruction, where when the executable instruction is being executed, the processor performs the following operation: sending a digital certificate revocation request to the blockchain, so that the blockchain determines a consensus verification result of a digital certificate of a target node, and determines, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain, where the digital certificate revocation request includes the digital certificate of the target node that is requested to be revoked.

[0028] The at least one technical solution used in the implementations of the present application can achieve the following beneficial effects:

[0029] In the solutions of the implementations of the present application, a function of a conventional CA center is implemented by the blockchain. When a node in the blockchain needs to apply for a digital certificate, the node can sign, by itself using the blockchain internal private key, to generate a to-be-verified digital certificate. The digital certificate can become an authorized and valid digital certificate only after the digital certificate is linked after consensus verification is passed in a blockchain network. The process of digital certificate issuing, verification, and storage is performed in the blockchain.

[0030] In the implementations of the present application, a digital certificate that passes consensus verification can be linked, and only a linked digital certificate is an authorized digital certificate. Therefore, even if a node is attacked by a hacker, or a hacker obtains a CA private key and can randomly issue a digital certificate, the hacker cannot obtain an authorized digital certificate in the blockchain, and therefore, cannot join the blockchain network to perform unauthorized communication. Therefore, based on advantages such as

decentralization, openness and transparency, and non-tampering, the digital certificate is managed by using the decentralized architecture to improve the security of the blockchain network.

#### BRIEF DESCRIPTION OF DRAWINGS

5 [0031] The accompanying drawings described here are intended to provide a further understanding of the present application, and constitute a part of the present application. The illustrative implementations of the present application and descriptions thereof are intended to describe the present application, and do not constitute improper limitations on the present application. In the accompanying drawings:

10 [0032] FIG 1 is a schematic flowchart illustrating a digital certificate management method, according to an implementation of the present application.

[0033] FIG. 2 is a schematic flowchart illustrating a second digital certificate management method, according to an implementation of the present application.

[0034] FIG 3 is a schematic flowchart illustrating a third digital certificate management method, according to an implementation of the present application.

15 [0035] FIG 4 is a schematic diagram illustrating an implementation scenario, according to an implementation of the present application.

[0036] FIG 5 is a schematic structural diagram illustrating a digital certificate management apparatus, according to an implementation of the present application.

20 [0037] FIG. 6 is a schematic structural diagram illustrating an electronic device, according to an implementation of the present application.

[0038] FIG 7 is a schematic structural diagram illustrating a second digital certificate management apparatus, according to an implementation of the present application.

[0039] FIG 8 is a schematic structural diagram illustrating a second electronic device, according to an implementation of the present application.

25 [0040] FIG 9 is a schematic structural diagram illustrating a third digital certificate management apparatus, according to an implementation of the present application.

[0041] FIG 10 is a schematic structural diagram illustrating a third electronic device, according to an implementation of the present application.

30 [0042] FIG 11 is a schematic structural diagram illustrating a fourth digital certificate management apparatus, according to an implementation of the present application.

[0043] FIG 12 is a schematic structural diagram illustrating a fourth electronic device, according to an implementation of the present application.

[0044] FIG 13 is a flowchart illustrating an example of a computer-implemented method for validating digital certificate of a node, according to an implementation of the present disclosure.

## DESCRIPTION OF EMBODIMENTS

[0045] To make the objectives, technical solutions, and advantages of the present application clearer, the following clearly and comprehensively describes the technical solutions of the present application with reference to the specific implementations and the corresponding accompanying drawings of the present application. Apparently, the described implementations are some rather than all of the implementations of the present application. Other implementations obtained by a person of ordinary skill in the art based on the implementations of the present application without creative efforts shall fall within the protection scope of the present application.

[0046] The technical solutions provided by the implementations of the present application are described in detail below with reference to the accompanying drawings.

[0047] Referring to FIG 1, an implementation of the present application provides a digital certificate management method, including the following steps:

[0048] S101: Receive a digital certificate linking request sent by a node in a blockchain, where the digital certificate linking request includes a to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain.

[0049] S103: Determine a consensus verification result of the to-be-verified digital certificate of the node.

[0050] S105: Determine, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain.

[0051] It can be understood that the node that sends the digital certificate linking request in the blockchain can be any node that wants to apply for a digital certificate in the blockchain. In the implementations of the present application, the node can sign, by itself using a private key disclosed in the blockchain, to generate the to-be-verified digital certificate, and further send the digital certificate linking request including the to-be-verified

digital certificate. So that the blockchain can be requested to write the to-be-verified digital certificate into the blockchain. In specific implementations, the node can send the digital certificate linking request in a network-wide broadcast method.

**[0052]** The to-be-verified digital certificate that is independently issued by the node is not validated before the digital certificate is linked, but it is not different from an authorized and validated digital certificate in content and form. In the implementations of the present application, the to-be-verified digital certificate can be represented by a series of digits indicating identity information of a correspondent node, and can include content including a version number of the certificate, information about a certificate holder (for example, can be represented by identity information of a node corresponding to the certificate), information about a certificate issuer (can be the same as the information about the certificate holder here, or can reflect a source of the private key), a validity period of the certificate, a serial number of the certificate, a signature of the certificate issuer, etc.

**[0053]** The to-be-verified digital certificate that is independently issued by the node is not validated. Only a digital certificate written into the blockchain is an authorized digital certificate, and only a node corresponding to the authorized digital certificate can normally participate in communication of the blockchain. Therefore, in the implementations of the present application, even if the private key required for issuing the certificate is disclosed, it will not cause disorder in the management of the digital certificate management, and will not affect the security of a blockchain network. On the contrary, the authorized digital certificate is generated based on the blockchain performing step S103 to perform consensus verification of the entire network, so that the security of the blockchain network is improved.

**[0054]** After receiving the digital certificate linking request, the blockchain can parse the request to obtain the to-be-verified digital certificate included in the request. Then consensus verification is performed on the to-be-verified digital certificate of the node. It can be understood that consensus verification means that each node in the blockchain can participate in verification of the to-be-verified digital certificate, and the consensus verification result is determined based on a consensus mechanism of the blockchain.

**[0055]** Each node in the blockchain can perform specific verification based on a pre-agreed verification standard. Content for verification can be related to information in the to-be-verified digital certificate, for example, whether the validity period is expired, whether the serial number satisfies a requirement, whether identity information of an application node

satisfies a requirement, etc.

[0056] Because a network delay can exist in a point-to-point network, the nodes in the blockchain can receive the digital certificate linking request at different times and can respond to the request at different speeds. Therefore, a node having a high receiving speed and a high response speed in the blockchain has more opportunities to participate in consensus verification on the to-be-verified digital certificate.

[0057] After completing verification on the to-be-verified digital certificate, nodes participating in consensus verification in the blockchain can send verification results to the blockchain (that is, nodes of the blockchain) in the network-wide broadcast method.

10 Correspondingly, referring to FIG 2, that the blockchain performs step S103 to determine the consensus verification result of the to-be-verified digital certificate of the node can include the following steps.

[0058] S301: Determine verification results of nodes participating in consensus verification in the blockchain.

15 [0059] It can be understood that the verification result can be "passing the consensus verification", or "not passing the consensus verification". In addition, the present step can be performed after a predetermined time from the time of broadcasting the to-be-verified digital certificate, or can be performed in real time after the start of consensus verification, or can be determined periodically, or can be performed when the number of nodes participating in 20 consensus verification reaches a predetermined value. In the implementations of the present application, to obtain a consensus verification result that satisfies the consensus mechanism of the blockchain, each or a combination of steps S301 to S305 can be performed repeatedly, and is not limited in the implementations of the present application.

25 [0060] S303: Determine the number of the first nodes and/or the number of the second nodes in the nodes participating in consensus verification, where a verification result of the first node is passing the consensus verification, and a verification result of the second node is not passing the consensus verification.

30 [0061] Specifically, after the nodes participating in consensus verification broadcast respective verification results, the nodes can be classified, based on the verification results, into the first node whose verification result is "passing the consensus verification", and the second node whose verification result is "not passing the consensus verification". Further, either of the two types of nodes can be counted, or numbers of both the two types of nodes

can be counted together, to determine whether a condition agreed by the consensus mechanism to determine the consensus verification result is satisfied. When the number of nodes is determined, the absolute number of nodes can be counted. For example, assuming there are 10 nodes participating in consensus verification, and there are four first nodes and 5 six second nodes. Alternatively, the weighted number of nodes can be counted based on weights of the nodes during consensus verification (a specific weight can be determined based on the consensus mechanism of the blockchain). For example, assuming there are four nodes in total participating in consensus verification, the absolute number of the first nodes and the second nodes are both 2, weights of the two first nodes are respectively 0.5 and 1.2, 10 and weights of the two second nodes are respectively 2 and 4. A calculation expression of the number of first nodes is:  $1 \times 0.5 + 1 \times 1.2 = 1.7$ , and a calculation expression of the number of second nodes is:  $1 \times 2 + 1 \times 4 = 6$ .

15 [0062] S305: Determine the consensus verification result based on the number of first nodes and/or the number of second nodes.

[0063] It can be understood that based on different consensus mechanisms of the blockchain, the consensus verification result can be determined based on the number of first nodes whose verification results are "passing the consensus verification", or can be determined based on the number of second nodes whose verification results are "not passing the consensus verification", or can be determined based on the numbers of both the two types 20 of nodes. It is not limited in the implementations of the present application.

25 [0064] If the consensus verification result is determined based on the number of first nodes, it can be checked whether the number of first nodes satisfies one or more of the following conditions: the number of first nodes reaches a first predetermined threshold; a ratio of the number of first nodes to the number of nodes participating in consensus verification reaches a second predetermined threshold; and a ratio of the number of first nodes to the number of nodes in the blockchain reaches a third predetermined threshold.

30 [0065] It can be understood that based on different consensus mechanisms of the blockchain, different conditions can be predetermined to determine the consensus verification result. All the previous three example aspects can reflect that the number of first nodes reaching a certain degree indicates that verification results of the to-be-verified digital certificate obtained by enough (specific standards can be different based on different consensus mechanisms) nodes in the blockchain are "passing the consensus verification".

Therefore, if the previous conditions are satisfied, the result of the consensus verification can be considered as "passing the consensus verification". This result can be understood as there are enough nodes in the blockchain consider the to-be-verified digital certificate that requests to be linked is authorized. Therefore, the to-be-verified digital certificate can be further 5 written into the blockchain, so that the authorized digital certificate is stored in the blockchain, and the node corresponding to the digital certificate can perform normal communication in the blockchain.

[0066] If the consensus verification result is determined based on the number of second nodes, if verification results of the to-be-verified digital certificate obtained by enough 10 (similarly, specific standards can be different based on different consensus mechanisms) nodes are "not passing the consensus verification", it indicates that enough nodes in the blockchain consider that the to-be-verified digital certificate that requests to be linked is unauthorized. Therefore, the to-be-verified digital certificate cannot be written into the blockchain to become an authorized digital certificate. Correspondingly, the node 15 corresponding to the to-be-verified digital certificate cannot participate in communication of the blockchain network. It can be understood that a specific standard of determining the consensus verification result based on the number of second nodes can be similar to the previous example, and depends on the consensus mechanism of the blockchain. Details are not described here again.

20 [0067] Corresponding to the implementation executed by the blockchain, an implementation of the present application further provides a digital certificate management method, which is performed by a node applying for a digital certificate, and can include:

[0068] A node in a blockchain sends a digital certificate linking request to the blockchain, so that the blockchain determines a consensus verification result of a to-be-verified digital 25 certificate of the node, and determines, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain.

[0069] The digital certificate linking request includes the to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain.

30 [0070] All related descriptions in the previous implementation executed by the blockchain are applicable here, and are not described here again.

[0071] Digital certificate management performed by using the implementations of the

present application can include digital certificate revocation in addition to digital certificate issuing, verification, and linking. Referring to FIG 3, an implementation of the present application further provides a digital certificate management method, to revoke a linked authorized digital certificate by performing the following steps:

- 5 [0072] S201: Receive a digital certificate revocation request sent by a node in a blockchain, where the digital certificate revocation request includes a digital certificate of a target node that is requested to be revoked.
- [0073] S203: Determine a consensus verification result of the digital certificate of the target node.
- 10 [0074] S205: Determine, based on the consensus verification result, whether to revoke the digital certificate of the target node.
- [0075] Step S203 of determining a consensus verification result of the digital certificate of the target node can include: determining verification results of nodes participating in consensus verification in the blockchain; determining the number of first nodes and/or the 15 number of second nodes in the nodes participating in consensus verification, where a verification result of the first node is passing the consensus verification, and a verification result of the second node is not passing the consensus verification; and determining the consensus verification result based on the number of first nodes and/or the number of second nodes.
- 20 [0076] Further, the determining the consensus verification result based on the number of first nodes includes: when the number of first nodes satisfies a first predetermined condition, determining that the consensus verification result is passing the consensus verification; and the first predetermined condition includes one or more of the following: the number of first nodes reaches a first predetermined threshold; a ratio of the number of first nodes to the 25 number of nodes participating in consensus verification reaches a second predetermined threshold; and a ratio of the number of first nodes to the number of nodes in the blockchain reaches a third predetermined threshold.
- [0077] The digital certificate of the target node is revoked in the blockchain when the consensus verification result is passing the consensus verification.
- 30 [0078] It can be understood that each node in the blockchain can initiate a digital certificate revocation request, can request to revoke a digital certificate of the node, or can request to revoke a digital certificate of another problematic node, which is not limited here.

In addition, it is not difficult to understand that in addition to the digital certificate of the target node that is requested to be revoked, the digital certificate revocation request can include a reason for revoking the digital certificate of the target node, so that each node participating in consensus verification in the blockchain determines whether the consensus 5 verification is passed.

[0079] It is worthwhile to note that when consensus verification is performed on the digital certificate revocation request, both the node that initiates the digital certificate revocation request and the target node can participate in consensus verification. However, when consensus verification is performed on a digital certificate linking request, a node that 10 initiates the request cannot participate in consensus verification, because the node has not obtained an authorized digital certificate, and cannot join a blockchain network.

[0080] It is worthwhile to further note that when consensus verification is performed on the digital certificate revocation request, the verification result of the first nodes being "passing the consensus verification" indicates that the first nodes agree to revoke the digital 15 certificate of the target node, and the verification result of the second nodes being "not passing the consensus verification" indicates that the second nodes disagree to revoke the digital certificate of the target node. Further, in the implementations, the consensus verification result can be determined based on the number of the first nodes and/or the number of the second nodes, to determine whether to revoke the digital certificate of the 20 target node. A process of determining the consensus verification result is similar to consensus verification on a to-be-verified digital certificate. The specific standard is determined by a consensus mechanism, and is not described here.

[0081] Corresponding to the implementation executed by the blockchain shown in FIG 3, an implementation of the present application further provides a digital certificate 25 management method, which is performed by a node applying for a digital certificate, and can include:

[0082] A node in a blockchain sends a digital certificate revocation request to the blockchain, so that the blockchain determines a consensus verification result of a digital certificate of a target node, and determines, based on the consensus verification result, 30 whether to revoke the digital certificate of the target node in the blockchain.

[0083] The digital certificate revocation request includes the digital certificate of the target node that is requested to be revoked.

[0084] All related descriptions in the previous implementation executed by the blockchain are applicable here, and are not described here again.

[0085] FIG 4 simply shows an information exchange process of digital certificate management in a blockchain network. For example, a process of digital certificate issuing, 5 verification, and linking includes the following steps:

[0086] S11: Node 4 is an initiation node and signs itself by using a disclosed private key, to generate a to-be-verified digital certificate.

[0087] S12: Node 4 broadcasts the generated to-be-verified digital certificate to a blockchain.

10 [0088] S13: Node 1, node 2, and node 3 sequentially participate in consensus verification on the to-be-verified digital certificate, and if a consensus verification result is "passing the consensus verification", each node (not limited to nodes 1 to 4) in the blockchain uses the to-be-verified digital certificate of node 4 as an authorized and valid digital certificate for linking. Therefore, node 4 obtains an authorized and valid digital certificate, and can 15 normally participate in communication of a blockchain network.

[0089] It can be understood that a digital certificate revocation process is similar to the process of digital certificate issuing, verification, and linking. The main difference is that a request sent by the initiation node changes from a digital certificate linking request to a digital certificate revocation request. Details are not described here again.

20 [0090] In the solution of the implementations of the present application, a function of a conventional CA center is implemented by the blockchain. When a node in the blockchain needs to apply for a digital certificate, the node can sign, by itself using the blockchain internal private key, to generate a to-be-verified digital certificate. The digital certificate can become an authorized and valid digital certificate only after the digital certificate is linked 25 after consensus verification is passed in the blockchain network. The process of digital certificate issuing, verification, and storage is performed in the blockchain. The digital certificate revocation process can also be performed in the blockchain.

[0091] In the implementations of the present application, a digital certificate that passes 30 consensus verification can be linked, and only a linked digital certificate is an authorized digital certificate. Therefore, even if a node is attacked by a hacker, or a hacker obtains a CA private key and can randomly issue a digital certificate, the hacker cannot obtain an authorized digital certificate in the blockchain, and therefore cannot join the blockchain

network to perform unauthorized communication. Therefore, based on advantages such as decentralization, openness and transparency, and non-tampering, the digital certificate is managed by using the decentralized architecture to improve the security of the blockchain network.

5 [0092] Referring to FIG 5, an implementation of the present application further provides a digital certificate management apparatus, where the apparatus is applied to a blockchain and includes: a request receiving module 101, configured to receive a digital certificate linking request sent by a node in the blockchain, where the digital certificate linking request includes a to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain; a consensus verification result determining module 103, configured to determine a consensus verification result of the to-be-verified digital certificate of the node; and a certificate management module 105, configured to determine, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain.

10 15 [0093] FIG 6 is a schematic structural diagram illustrating an electronic device, according to an implementation of the present application. Referring to FIG 6, in terms of hardware, the electronic device includes a processor, and optionally further includes an internal bus, a network interface, and a storage. The storage can include a memory, for example, a high-speed random access memory (RAM), and can further include a nonvolatile memory (nonvolatile memory), for example, at least one magnetic disk storage. Certainly, the electronic device can further include hardware needed by another service.

20 25 [0094] The processor, the network interface, and the storage can be connected to each other by using the internal bus. The internal bus can be an industry standard architecture (ISA) bus, a Peripheral Component Interconnect (PCI) bus, an extended industry standard architecture (EISA) bus, etc. The bus can be classified into an address bus, a data bus, a control bus, etc. For ease of indication, the bus is indicated by using only one double-headed arrow in FIG 6. However, it does not mean that there is only one bus or only one type of bus.

[0095] The storage is configured to store a program. The program can include program code, and the program code includes computer operation instructions. The storage can include a memory and a nonvolatile memory, and provide an instruction and data for the processor.

30 [0096] The processor reads a corresponding computer program from the nonvolatile

memory to the memory for running, and a digital certificate management apparatus is logically formed. The processor executes the program stored in the storage, and is configured to perform the following operations: receiving a digital certificate linking request sent by a node in a blockchain, where the digital certificate linking request includes a to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain; determining a consensus verification result of the to-be-verified digital certificate of the node; and determining, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain.

10 [0097] The previous method executed by the digital certificate management apparatus that is disclosed in the implementation shown in FIG 1 of the present application can be applied to the processor, or can be implemented by the processor. The processor can be an integrated circuit chip and have a signal processing capability. In an implementation process, steps in the previous method can be implemented by using a hardware integrated logical circuit in the processor, or by using instructions in a form of software. The processor can be a general purpose processor, including a central processing unit (CPU), a network processor (NP), etc.; or can be a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA) or another programmable logical device, a discrete gate or transistor logic device, a discrete hardware component, etc. The 15 processor can implement or perform the methods, the steps, and the logical block diagrams disclosed in the implementations of the present application. The general purpose processor can be a microprocessor, or the processor can be any conventional processor, etc. The steps of the methods disclosed in the implementations of the present application can be directly performed by a hardware decoding processor, or performed by a combination of hardware 20 and software modules in a decoding processor. The software module can be located in a mature storage medium in the field, such as a random access memory, a flash memory, a read-only memory, a programmable read-only memory, an electrically erasable programmable memory, or a register. The storage medium is located in the storage, and the processor reads information in the storage and completes the steps in the previous method in 25 combination with hardware in the processor.

30 [0098] The electronic device can further perform the method performed by the digital certificate management apparatus in FIG 1, and implement functions of the digital certificate

management apparatus in the implementation shown in FIG. 1. Details are not described in the implementations of the present application.

[0099] An implementation of the present application further provides a computer-readable storage medium, the computer-readable storage medium stores one or 5 more programs, and the one or more programs include an instruction. When the instruction is executed by an electronic device including a plurality of application programs, the electronic device can execute the method executed by a digital certificate management apparatus in the implementation shown in FIG. 1, and is configured to perform the following operations: receiving a digital certificate linking request sent by a node in a blockchain, where the digital 10 certificate linking request includes a to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain; determining a consensus verification result of the to-be-verified digital certificate of the node; and determining, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain.

[00100] Referring to FIG. 7, an implementation of the present application further provides a digital certificate management apparatus, where the apparatus is applied to a blockchain and includes: a request receiving module 201, configured to receive a digital certificate revocation request sent by a node in the blockchain, where the digital certificate revocation request includes a digital certificate of a target node that is requested to be revoked; a 20 consensus verification result determining module 203, configured to determine a consensus verification result of the digital certificate of the target node; and a certificate management module 205, configured to determine, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain.

[0100] FIG. 8 is a schematic structural diagram illustrating an electronic device, 25 according to an implementation of the present application. Referring to FIG. 8, in terms of hardware, the electronic device includes a processor, and optionally further includes an internal bus, a network interface, and a storage. The storage can include a memory, for example, a high-speed random access memory (RAM), and can further include a nonvolatile memory (nonvolatile memory), for example, at least one magnetic disk storage. Certainly, the 30 electronic device can further include hardware needed by another service.

[0101] The processor, the network interface, and the storage can be connected to each other by using the internal bus. The internal bus can be an industry standard architecture (ISA)

bus, a Peripheral Component Interconnect (PCI) bus, an extended industry standard architecture (EISA) bus, etc. The bus can be classified into an address bus, a data bus, a control bus, etc. For ease of indication, the bus is indicated by using only one double-headed arrow in FIG 8. However, it does not mean that there is only one bus or only one type of bus.

5 [0102] The storage is configured to store a program. The program can include program code, and the program code includes computer operation instructions. The storage can include a memory and a nonvolatile memory, and provide an instruction and data for the processor.

10 [0103] The processor reads a corresponding computer program from the nonvolatile memory to the memory for running, and a digital certificate management apparatus is logically formed. The processor executes the program stored in the storage, and is configured to perform the following operations: receiving a digital certificate revocation request sent by a node in a blockchain, where the digital certificate revocation request includes a digital certificate of a target node that is requested to be revoked; determining a consensus 15 verification result of the digital certificate of the target node; and determining, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain.

20 [0104] The previous method executed by the digital certificate management apparatus that is disclosed in the implementation shown in FIG 3 of the present application can be applied to the processor, or can be implemented by the processor. The processor can be an integrated circuit chip and have a signal processing capability. In an implementation process, steps in the previous method can be implemented by using a hardware integrated logical circuit in the processor, or by using instructions in a form of software. The processor can be a general purpose processor, including a central processing unit (CPU), a network processor 25 (NP), etc.; or can be a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA) or another programmable logical device, a discrete gate or transistor logic device, a discrete hardware component, etc. The processor can implement or perform the methods, the steps, and the logical block diagrams disclosed in the implementations of the present application. The general purpose processor 30 can be a microprocessor, or the processor can be any conventional processor, etc. The steps of the methods disclosed in the implementations of the present application can be directly performed by a hardware decoding processor, or performed by a combination of hardware

and software modules in a decoding processor. The software module can be located in a mature storage medium in the field, such as a random access memory, a flash memory, a read-only memory, a programmable read-only memory, an electrically erasable programmable memory, or a register. The storage medium is located in the storage, and the 5 processor reads information in the storage and completes the steps in the previous method in combination with hardware in the processor.

10 [0105] The electronic device can further perform the method performed by the digital certificate management apparatus in FIG. 3, and implement functions of the digital certificate management apparatus in the implementation shown in FIG. 3. Details are not described in the implementations of the present application.

15 [0106] An implementation of the present application further provides a computer-readable storage medium, the computer-readable storage medium stores one or more programs, and the one or more programs include an instruction. When the instruction is executed by an electronic device including a plurality of application programs, the electronic device can execute the method executed by a digital certificate management apparatus in the implementation shown in FIG. 1, and is configured to perform the following operations: receiving a digital certificate revocation request sent by a node in a blockchain, where the digital certificate revocation request includes a digital certificate of a target node that is requested to be revoked; determining a consensus verification result of the digital certificate 20 of the target node; and determining, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain.

25 [0107] Referring to FIG. 9, an implementation of the present application provides a digital certificate management apparatus, where the apparatus is applied to a node in a blockchain and includes: a request initiation module 401, configured to send a digital certificate linking request to the blockchain, so that the blockchain determines a consensus verification result of a to-be-verified digital certificate of the node, and determines, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain, where the digital certificate linking request includes the to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to 30 request to write the to-be-verified digital certificate into the blockchain.

[0108] FIG. 10 is a schematic structural diagram illustrating an electronic device, according to an implementation of the present application. Referring to FIG. 10, in terms of

hardware, the electronic device includes a processor, and optionally further includes an internal bus, a network interface, and a storage. The storage can include a memory, for example, a high-speed random access memory (RAM), and can further include a nonvolatile memory (nonvolatile memory), for example, at least one magnetic disk storage. Certainly, the 5 electronic device can further include hardware needed by another service.

[0109] The processor, the network interface, and the storage can be connected to each other by using the internal bus. The internal bus can be an industry standard architecture (ISA) bus, a Peripheral Component Interconnect (PCI) bus, an extended industry standard architecture (EISA) bus, etc. The bus can be classified into an address bus, a data bus, a 10 control bus, etc. For ease of indication, the bus is indicated by using only one double-headed arrow in FIG 10. However, it does not mean that there is only one bus or only one type of bus.

[0110] The storage is configured to store a program. The program can include program code, and the program code includes computer operation instructions. The storage can 15 include a memory and a nonvolatile memory, and provide an instruction and data for the processor.

[0111] The processor reads a corresponding computer program from the nonvolatile memory to the memory for running, and a digital certificate management apparatus is logically formed. The processor executes the program stored in the storage, and is configured 20 to perform the following operation: sending a digital certificate linking request to a blockchain, so that the blockchain determines a consensus verification result of a to-be-verified digital certificate of a node, and determines, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain, where the digital certificate linking request includes the to-be-verified digital certificate that 25 is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain.

[0112] The previous methods executed by the digital certificate management apparatus that are disclosed in the previous implementations of the present application can be applied to the processor, or can be implemented by the processor. The processor can be an integrated 30 circuit chip and have a signal processing capability. In an implementation process, steps in the previous methods can be implemented by using a hardware integrated logical circuit in the processor, or by using instructions in a form of software. The processor can be a general

purpose processor, including a central processing unit (CPU), a network processor (NP), etc.; or can be a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA) or another programmable logical device, a discrete gate or transistor logic device, a discrete hardware component, etc. The processor can 5 implement or perform the methods, the steps, and the logical block diagrams disclosed in the implementations of the present application. The general purpose processor can be a microprocessor, or the processor can be any conventional processor, etc. The steps of the methods disclosed in the implementations of the present application can be directly performed by a hardware decoding processor, or performed by a combination of hardware 10 and software modules in a decoding processor. The software module can be located in a mature storage medium in the field, such as a random access memory, a flash memory, a read-only memory, a programmable read-only memory, an electrically erasable programmable memory, or a register. The storage medium is located in the storage, and the processor reads information in the storage and completes the steps in the previous methods in 15 combination with hardware in the processor.

[0113] The electronic device can further perform the method performed by the digital certificate management apparatus, and implement functions of the digital certificate management apparatus in the previous implementations. Details are not described in the implementations of the present application.

20 [0114] An implementation of the present application further provides a computer-readable storage medium, the computer-readable storage medium stores one or more programs, and the one or more programs include an instruction. When the instruction is executed by an electronic device including a plurality of application programs, the electronic device can execute the methods executed by a digital certificate management apparatus in the previous implementations, and is configured to perform the following operation: sending a digital certificate linking request to a blockchain, so that the blockchain determines a consensus verification result of a to-be-verified digital certificate of a node, and determines, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain, where the digital certificate linking request includes the 25 to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain.

30

[0115] Referring to FIG 11, an implementation of the present application further provides a digital certificate management apparatus, where the apparatus is applied to a node in a blockchain and includes: a request initiation module 501, configured to send a digital certificate revocation request to the blockchain, so that the blockchain determines a consensus verification result of a digital certificate of a target node, and determines, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain, where the digital certificate revocation request includes the digital certificate of the target node that is requested to be revoked.

[0116] FIG 12 is a schematic structural diagram illustrating an electronic device, according to an implementation of the present application. Referring to FIG 12, in terms of hardware, the electronic device includes a processor, and optionally further includes an internal bus, a network interface, and a storage. The storage can include a memory, for example, a high-speed random access memory (RAM), and can further include a nonvolatile memory, for example, at least one magnetic disk storage. Certainly, the electronic device can further include hardware needed by another service.

[0117] The processor, the network interface, and the storage can be connected to each other by using the internal bus. The internal bus can be an industry standard architecture (ISA) bus, a Peripheral Component Interconnect (PCI) bus, an extended industry standard architecture (EISA) bus, etc. The bus can be classified into an address bus, a data bus, a control bus, etc. For ease of indication, the bus is indicated by using only one double-headed arrow in FIG 12. However, it does not mean that there is only one bus or only one type of bus.

[0118] The storage is configured to store a program. The program can include program code, and the program code includes computer operation instructions. The storage can include a memory and a nonvolatile memory, and provide an instruction and data for the processor.

[0119] The processor reads a corresponding computer program from the nonvolatile memory to the memory for running, and a digital certificate management apparatus is logically formed. The processor executes the program stored in the storage, and is configured to perform the following operation: sending a digital certificate revocation request to a blockchain, so that the blockchain determines a consensus verification result of a digital certificate of a target node, and determines, based on the consensus verification result,

whether to revoke the digital certificate of the target node in the blockchain, where the digital certificate revocation request includes the digital certificate of the target node that is requested to be revoked.

[0120] The previous methods executed by the digital certificate management apparatus that are disclosed in the previous implementations of the present application can be applied to the processor, or can be implemented by the processor. The processor can be an integrated circuit chip and have a signal processing capability. In an implementation process, steps in the previous methods can be implemented by using a hardware integrated logical circuit in the processor, or by using instructions in a form of software. The processor can be a general purpose processor, including a central processing unit (CPU), a network processor (NP), etc.; or can be a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA) or another programmable logical device, a discrete gate or transistor logic device, a discrete hardware component, etc. The processor can implement or perform the methods, the steps, and the logical block diagrams disclosed in the implementations of the present application. The general purpose processor can be a microprocessor, or the processor can be any conventional processor, etc. The steps of the methods disclosed in the implementations of the present application can be directly performed by a hardware decoding processor, or performed by a combination of hardware and software modules in a decoding processor. The software module can be located in a mature storage medium in the field, such as a random access memory, a flash memory, a read-only memory, a programmable read-only memory, an electrically erasable programmable memory, or a register. The storage medium is located in the storage, and the processor reads information in the storage and completes the steps in the previous methods in combination with hardware in the processor.

[0121] The electronic device can further perform the method performed by the digital certificate management apparatus, and implement functions of the digital certificate management apparatus in the previous implementations. Details are not described in the implementations of the present application.

[0122] An implementation of the present application further provides a computer-readable storage medium, the computer-readable storage medium stores one or more programs, and the one or more programs include an instruction. When the instruction is executed by an electronic device including a plurality of application programs, the electronic

device can execute the methods executed by a digital certificate management apparatus in the previous implementations, and is configured to perform the following operation: sending a digital certificate revocation request to a blockchain, so that the blockchain determines a consensus verification result of a digital certificate of a target node, and determines, based on 5 the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain, where the digital certificate revocation request includes the digital certificate of the target node that is requested to be revoked.

[0123] A person skilled in the art should understand that the implementations of the present disclosure can be provided as a method, a system, or a computer program product. 10 Therefore, the present disclosure can use a form of hardware only implementations, software only implementations, or implementations with a combination of software and hardware. Moreover, the present disclosure can use a form of a computer program product that is implemented on one or more computer-readable storage media (including but not limited to a magnetic disk storage, a CD-ROM, an optical memory, etc.) that include computer-readable 15 program code.

[0124] The present disclosure is described with reference to the flowcharts and/or block diagrams of the method, the device (system), and the computer program product according to the implementations of the present disclosure. It should be understood that computer program instructions can be used to implement each process and/or each block in the flowcharts and/or 20 the block diagrams and a combination of a process and/or a block in the flowcharts and/or the block diagrams. These computer program instructions can be provided for a general-purpose computer, a dedicated computer, an embedded processor, or a processor of another programmable data processing device to generate a machine, so that the instructions executed by the computer or the processor of the another programmable data processing device 25 generate an apparatus for implementing a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0125] These computer program instructions can be stored in a computer-readable memory that can instruct the computer or the another programmable data processing device to work in a specific method, so that the instructions stored in the computer-readable memory generate an artifact that includes an instruction apparatus. The instruction apparatus implements a specific function in one or more processes in the flowcharts and/or in one or 30 more blocks in the block diagrams.

[0126] These computer program instructions can be loaded onto the computer or the another programmable data processing device, so that a series of operations and steps are performed on the computer or the another programmable device, thereby generating computer-implemented processing. Therefore, the instructions executed on the computer or 5 the another programmable device provide steps for implementing a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0127] In typical configuration, a computing device includes one or more processors (CPU), an input/output interface, a network interface, and a memory.

[0128] The memory can include a nonpersistent storage, a random access memory (RAM), a nonvolatile memory, and/or another form that are in a computer-readable medium, 10 for example, a read-only memory (ROM) or a flash memory (flash memory). The memory is an example of the computer-readable medium.

[0129] The computer-readable medium includes persistent, nonpersistent, movable, and 15 unmovable media that can implement information storage by using any method or technology. Information can be a computer-readable instruction, a data structure, a program module, or other data. An example of a computer storage medium includes but is not limited to a parameter random access memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), another type of random access memory (RAM), a 20 read-only memory (ROM), an electrically erasable programmable read only memory (EEPROM), a flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or other optical storage, a cassette magnetic tape, tape and disk storage or another magnetic storage device or any other non-transmission media that can be configured to store information that can be accessed by 25 the computing device. Based on the definition in the present specification, the computer-readable medium does not include a transitory computer-readable media (transitory computer-readable media), for example, a modulated data signal and carrier.

[0130] It is worthwhile to further note that in the present specification, the terms "include", "comprise", or their any other variant is intended to cover a non-exclusive inclusion, so that a process, a method, an article, or a device that includes a list of elements 30 not only includes those elements but also includes other elements which are not expressly listed, or further includes elements inherent to such process, method, article, or device. An element preceded by "includes a ..." does not, without more constraints, preclude the

existence of additional identical elements in the process, method, article, or device that includes the element.

[0131] A person skilled in the art should understand that the implementations of the present application can be provided as a method, a system, or a computer program product.

5 Therefore, the present application can use a form of hardware only implementations, software only implementations, or implementations with a combination of software and hardware. Moreover, the present application can use a form of a computer program product that is implemented on one or more computer-readable storage media (including but not limited to a magnetic disk storage, a CD-ROM, an optical memory, etc.) that include computer-readable program code.

10 [0132] The previous descriptions are merely implementations of the present application, and are not intended to limit the present application. For a person skilled in the art, the present application can have various modifications and changes. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle 15 of the present application shall fall within the scope of the claims of the present application.

[0133] FIG 13 is a flowchart illustrating an example of a computer-implemented method 1300 for validating digital certificate of a node, according to an implementation of the present disclosure. For clarity of presentation, the description that follows generally describes method 1300 in the context of the other figures in this description. For example, the method 1300 can 20 be implemented by a blockchain node described with reference to FIG 4, the digital certificate management apparatus of FIG 5, or any other computing device in communication with blockchain nodes. However, it will be understood that method 1300 can be performed, for example, by any system, environment, software, and hardware, or a combination of 25 systems, environments, software, and hardware, as appropriate. In some implementations, various steps of method 1300 can be run in parallel, in combination, in loops, or in any order.

[0134] At 1302, a linking request is received from a node. The linking request includes a request to link the node to a blockchain network. Node 4 in FIG. 4 is an example of a node sending the linking request. The node can include a digital code into the linking request. In 30 case the linking request is approved, a digital certificate is assigned to the node based on the digital code. The digital code can be in a form of a digital certificate that is yet to be approved. The node may provide the digital certificate based on a private key associated with the node. The node sends the request to the blockchain network. For example, the node may send the

request a set of blockchain nodes (for example, nodes 1-3 in FIG. 4), or to a digital certificate management device (for example, a CA) that forwards the linking request to a set of blockchain nodes for consensus verification. From 1302, method 1300 proceeds to 1304.

**[0135]** At 1304, one or more consensus verification messages are received from blockchain nodes approving or denying the links. For example, each node in the set of blockchain nodes that received the linking request may send out an approval or denial of the request in form of a consensus verification message. Nodes of the set of blockchain nodes send the consensus verification message to each other, a digital certificate management device of the blockchain, or a combination of the nodes of the set of blockchain nodes and the digital certificate management device of the blockchain. In some implementations, number of nodes in the set of blockchain nodes need to be greater than a threshold number. In some examples, the threshold number is determined based on a total number of all nodes in the blockchain. For example, the threshold may be 60% (or 30%) of the total number of nodes. From 1304, method 1300 proceeds to 1306.

**[0136]** At 1306, a consensus verification result is determined based on the consensus verification messages received from the set of blockchain nodes. The consensus verification result can be determined based on the number of nodes in the set of blockchain nodes. For example, the consensus verification result can be determined based on a majority, or a ratio of approval and denial consensus verification messages received from the set of blockchain nodes. In some implementations, one or more blockchain nodes are associated with a weight, and the consensus verification result is determined based on the weight of the respective nodes. For example, between two nodes with different weights, the node with a greater weight can influence the consensus verification result more than the other node. The consensus verification result indicates whether the set of blockchain nodes have approved or denied the linking request. From 1306, method 1300 proceeds to 1308.

**[0137]** At 1308, a determination is made as to whether the linking request is approved. The determination is made based on the consensus verification result. In some examples, the linking request is determined to be approved based on determining that number of blockchain nodes that approve the linking request is higher than a threshold number. In some examples, the linking request is determined to be approved based on determining that a ratio of the number of blockchain nodes that approve the linking request to the number of blockchain nodes that provided the consensus verification message is higher than a threshold number. In

some examples, the linking request is determined to be approved based on determining that ratio of number of blockchain nodes that approve the linking request to number of all blockchain nodes in the blockchain network is higher than a threshold number. If it is determined that the linking request is approved, method 1300 proceeds to 1310. Otherwise, if 5 it is determined that the linking request is not approved (or denied), method 1300 proceeds to 1312.

[0138] At 1310, a digital certificate associated with the node (which is the requesting node) is stored in the blockchain. Once the blockchain approves the linking request, the node is added (or linked) to the blockchain and a digital certificate associated with the node is 10 stored into the blockchain. The digital certificate can be provided based on the digital code included in the linking request. The digital certificate can be stored into the blockchain nodes (for example, multiple nodes of the blockchain), into a digital certificate management device (for example, a CA) associated with the blockchain, or both.

[0139] At 1312, the linking request is rejected. Upon rejecting the linking request, no 15 digital certificate is assigned to the node and the node is not added to the blockchain. In some implementations, a history of the rejected linking requests or digital codes included in the rejected linking are stored in the blockchain (for example, in multiple blockchain nodes).

[0140] Method 1300 provides an example method for validating digital certificates 20 blockchain nodes. In some implementations, digital certificates can be revoked by blockchain nodes. For example, a node of the blockchain may request revocation of a digital certificate that is already valid in the blockchain. The node can send a revocation request for revoking its own digital certificate, or another node's digital certificate. The revocation request can include a digital certificate or another identifier of a targeted node that is requested to be revoked. The revocation request can also include a reason for the request, for example, an 25 indication that the targeted node conducted insecure transactions within the blockchain.

[0141] Similar to the validation process, the revocation process is performed based on a 30 consensus verification received from a set of blockchain nodes. Accordingly, one or more revocation consensus messages are received from one or more blockchain nodes; each of the revocation consensus messages indicating whether the respective blockchain node approves or denies the revocation request. Based on the received revocation consensus messages, a revocation consensus result is determined. The revocation consensus result indicates whether the revocation request has been approved or denied by the one or more blockchain nodes.

Upon determining that the revocation consensus result has been approved, the digital certificate of the targeted node is revoked from digital certificates stored in the blockchain network. A node whose digital certificate is revoked loses connection to the blockchain. If the node wants to reconnect (or link) to the blockchain, the node has to send a linking request to the blockchain. In some implementations, a list of the revoked digital certificates is stored in the blockchain. For example, multiple nodes (for example, the one or more nodes that have approved the revocation) may store the revoked digital certificate or another identifier of the targeted node into a revocation list.

[0142] To ensure security in blockchain communications, each blockchain node is assigned with a digital certificate. Only the nodes that have a valid digital certificate are authorized to communicate in the blockchain. Conventionally, the digital certificates are assigned to the nodes by a CA. The CA provides the digital certificates based on a private key associated with the blockchain. The CA stores information of the issued, revoked, and valid digital certificates. When nodes in the blockchain need to communicate with each other, validity of the digital certificates of the respective nodes are checked by querying the digital certificates in the CA.

[0143] The conventional dependency on CA for issuance, revocation, and validity check of the digital certificates puts the blockchain communications at risk and exposed to hackers' manipulations. Once the CA is hacked, a hacker can tamper with the digital certificate validities stored in the CA. For example, the hacker can revoke digital certificates of one or more authorized nodes, or validate digital certificates for one or more previously revoked nodes. In addition, the hacker can add unauthorized nodes to the blockchain by including fake digital certificates into the CA.

[0144] Implementations of the present disclosure provide techniques to improve security of blockchain. According to the implementations, validation, revocation, or storing of the digital certificates are performed by the nodes of the blockchain, rather than (or in addition to) the CA. A digital certificate is validated only after multiple blockchain nodes pass a consensus verification, approving the node to be linked to the blockchain. Similarly, a digital certificate is revoked only when multiple blockchain nodes pass a consensus verification, approving revocation of digital certificate of the node. Further, the validity (or revocation) of the blockchain nodes is stored in multiple nodes, rather than only on a CA. Accordingly, even if a node or the CA is attacked by a hacker, the hacker cannot arbitrarily issue, revoke, or

manipulate validity of digital certificates of the blockchain nodes without receiving an approval of blockchain nodes.

[0145] Embodiments and the operations described in this specification can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware, 5 including the structures disclosed in this specification or in combinations of one or more of them. The operations can be implemented as operations performed by a data processing apparatus on data stored on one or more computer-readable storage devices or received from other sources. A data processing apparatus, computer, or computing device may encompass 10 apparatus, devices, and machines for processing data, including by way of example a programmable processor, a computer, a system on a chip, or multiple ones, or combinations, of the foregoing. The apparatus can include special purpose logic circuitry, for example, a central processing unit (CPU), a field programmable gate array (FPGA) or an application-specific integrated circuit (ASIC). The apparatus can also include code that creates an execution environment for the computer program in question, for example, code 15 that constitutes processor firmware, a protocol stack, a database management system, an operating system (for example an operating system or a combination of operating systems), a cross-platform runtime environment, a virtual machine, or a combination of one or more of them. The apparatus and execution environment can realize various different computing model infrastructures, such as web services, distributed computing and grid computing 20 infrastructures.

[0146] A computer program (also known, for example, as a program, software, software application, software module, software unit, script, or code) can be written in any form of 25 programming language, including compiled or interpreted languages, declarative or procedural languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, object, or other unit suitable for use in a computing environment. A program can be stored in a portion of a file that holds other programs or data (for example, one or more scripts stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (for example, files that 30 store one or more modules, sub-programs, or portions of code). A computer program can be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

[0147] Processors for execution of a computer program include, by way of example, both

general- and special-purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read-only memory or a random-access memory or both. The essential elements of a computer are a processor for performing actions in accordance with instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data. A computer can be embedded in another device, for example, a mobile device, a personal digital assistant (PDA), a game console, a Global Positioning System (GPS) receiver, or a portable storage device. Devices suitable for storing computer program instructions and data include non-volatile memory, media and memory devices, including, by way of example, semiconductor memory devices, magnetic disks, and magneto-optical disks. The processor and the memory can be supplemented by, or incorporated in, special-purpose logic circuitry.

**[0148]** Mobile devices can include handsets, user equipment (UE), mobile telephones (for example, smartphones), tablets, wearable devices (for example, smart watches and smart eyeglasses), implanted devices within the human body (for example, biosensors, cochlear implants), or other types of mobile devices. The mobile devices can communicate wirelessly (for example, using radio frequency (RF) signals) to various communication networks (described below). The mobile devices can include sensors for determining characteristics of the mobile device's current environment. The sensors can include cameras, microphones, proximity sensors, GPS sensors, motion sensors, accelerometers, ambient light sensors, moisture sensors, gyroscopes, compasses, barometers, fingerprint sensors, facial recognition systems, RF sensors (for example, Wi-Fi and cellular radios), thermal sensors, or other types of sensors. For example, the cameras can include a forward- or rear-facing camera with movable or fixed lenses, a flash, an image sensor, and an image processor. The camera can be a megapixel camera capable of capturing details for facial and/or iris recognition. The camera along with a data processor and authentication information stored in memory or accessed remotely can form a facial recognition system. The facial recognition system or one-or-more sensors, for example, microphones, motion sensors, accelerometers, GPS sensors, or RF sensors, can be used for user authentication.

**[0149]** To provide for interaction with a user, embodiments can be implemented on a computer having a display device and an input device, for example, a liquid crystal display

(LCD) or organic light-emitting diode (OLED)/virtual-reality (VR)/augmented-reality (AR) display for displaying information to the user and a touchscreen, keyboard, and a pointing device by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user 5 can be any form of sensory feedback, for example, visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, or tactile input. In addition, a computer can interact with a user by sending documents to and receiving documents from a device that is used by the user; for example, by sending web pages to a web browser on a user's client device in response to requests received from 10 the web browser.

**[0150]** Embodiments can be implemented using computing devices interconnected by any form or medium of wireline or wireless digital data communication (or combination thereof), for example, a communication network. Examples of interconnected devices are a client and a server generally remote from each other that typically interact through a 15 communication network. A client, for example, a mobile device, can carry out transactions itself, with a server, or through a server, for example, performing buy, sell, pay, give, send, or loan transactions, or authorizing the same. Such transactions may be in real time such that an action and a response are temporally proximate; for example an individual perceives the action and the response occurring substantially simultaneously, the time difference for a 20 response following the individual's action is less than 1 millisecond (ms) or less than 1 second (s), or the response is without intentional delay taking into account processing limitations of the system.

**[0151]** Examples of communication networks include a local area network (LAN), a radio access network (RAN), a metropolitan area network (MAN), and a wide area network (WAN). The communication network can include all or a portion of the Internet, another 25 communication network, or a combination of communication networks. Information can be transmitted on the communication network according to various protocols and standards, including Long Term Evolution (LTE), 5G IEEE 802, Internet Protocol (IP), or other protocols or combinations of protocols. The communication network can transmit voice, 30 video, biometric, or authentication data, or other information between the connected computing devices.

**[0152]** Features described as separate implementations may be implemented, in

combination, in a single implementation, while features described as a single implementation may be implemented in multiple implementations, separately, or in any suitable sub-combination. Operations described and claimed in a particular order should not be understood as requiring that the particular order, nor that all illustrated operations must be 5 performed (some operations can be optional). As appropriate, multitasking or parallel-processing (or a combination of multitasking and parallel-processing) can be performed.

## CLAIMS

What is claimed is:

1. A method for digital certificate management, the method comprising:

receiving a digital certificate linking request sent by a node in a blockchain, wherein  
5 the digital certificate linking request comprises a to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain (S101);

determining a consensus verification result of the to-be-verified digital certificate of the node (S103); and

10 determining, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain (S105).

2. The method according to claim 1, wherein determining the consensus verification result of the to-be-verified digital certificate of the node comprises:

15 determining verification results of nodes participating in consensus verification in the blockchain (S301);

determining the number of first nodes and/or the number of second nodes in the nodes participating in consensus verification, wherein a verification result of the first node is passing the consensus verification, and a verification result of the second node is not passing the consensus verification (S303); and

20 determining the consensus verification result based on the number of first nodes and/or the number of second nodes (S305).

3. The method according to claim 2, wherein determining the consensus verification result based on the number of first nodes comprises:

25 when the number of first nodes satisfies a first predetermined condition, determining that the consensus verification result is passing the consensus verification; and

the first predetermined condition comprises one or more of the following:

the number of first nodes reaches a first predetermined threshold,

a ratio of the number of first nodes to the number of nodes participating in consensus verification reaches a second predetermined threshold, and

30 a ratio of the number of first nodes to the number of nodes in the blockchain reaches a third predetermined threshold.

4. The method according to claim 3, wherein determining, based on the consensus verification result, whether to write the to-be-verified digital certificate into the blockchain comprises:

5 writing the to-be-verified digital certificate into the blockchain when the consensus verification result is passing the consensus verification.

5. The method according to any one of claims 1 to 4, further comprising:

receiving a digital certificate revocation request sent by the node in the blockchain, wherein the digital certificate revocation request comprises a digital certificate of a target node that is requested to be revoked (S201);

10 determining a consensus verification result of the digital certificate of the target node (S203); and

determining, based on the consensus verification result, whether to revoke the digital certificate of the target node (S205).

6. The method according to any one of claims 1 to 5, further comprising:

15 receiving a digital certificate revocation request sent by a node in a blockchain, wherein the digital certificate revocation request comprises a digital certificate of a target node that is requested to be revoked;

determining a consensus verification result of the digital certificate of the target node; and

20 determining, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain.

7. The method according to claim 6, wherein the determining, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain comprises:

25 revoking the digital certificate of the target node in the blockchain when the consensus verification result is passing the consensus verification.

8. The method according to any one of claims 1 to 7, further comprising:

sending, by a node in a blockchain, a digital certificate linking request to the blockchain, so that the blockchain determines a consensus verification result of a to-be-verified digital certificate of the node, and determines, based on the consensus

verification result, whether to write the to-be-verified digital certificate into the blockchain, wherein the digital certificate linking request comprises the to-be-verified digital certificate that is generated by the node through signing by using a private key, and is used to request to write the to-be-verified digital certificate into the blockchain.

5 9. The method according to any one of claims 1 to 8, further comprising:

sending, by a node in a blockchain, a digital certificate revocation request to the blockchain, so that the blockchain determines a consensus verification result of a digital certificate of a target node, and determines, based on the consensus verification result, whether to revoke the digital certificate of the target node in the blockchain, wherein the 10 digital certificate revocation request comprises the digital certificate of the target node that is requested to be revoked.

10. The method according to any one of claims 1 to 9, wherein the digital certificate comprises at least one of a version, a serial number, an issuer information, a validity period, and a signature of issuer.

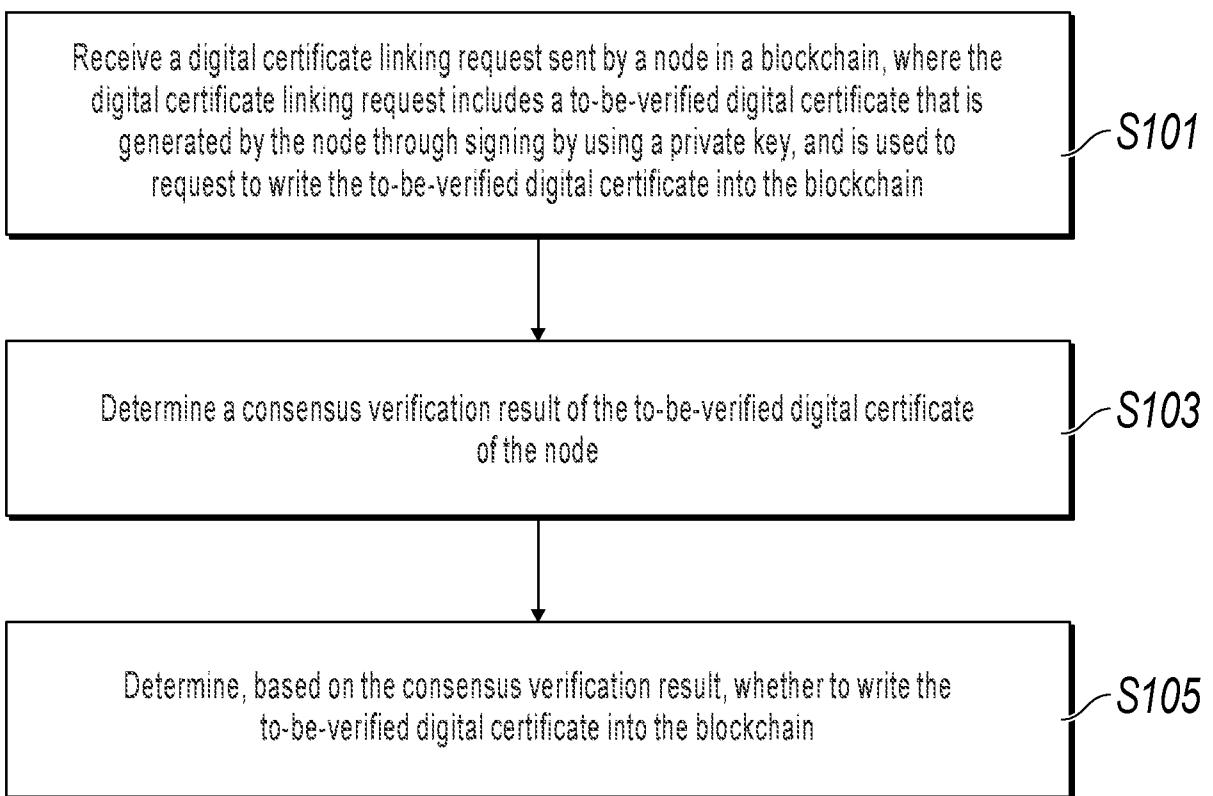
15 11. The method according to any one of claims 1 to 10, wherein the digital certificate is unauthorized before being chained in the node of the blockchain.

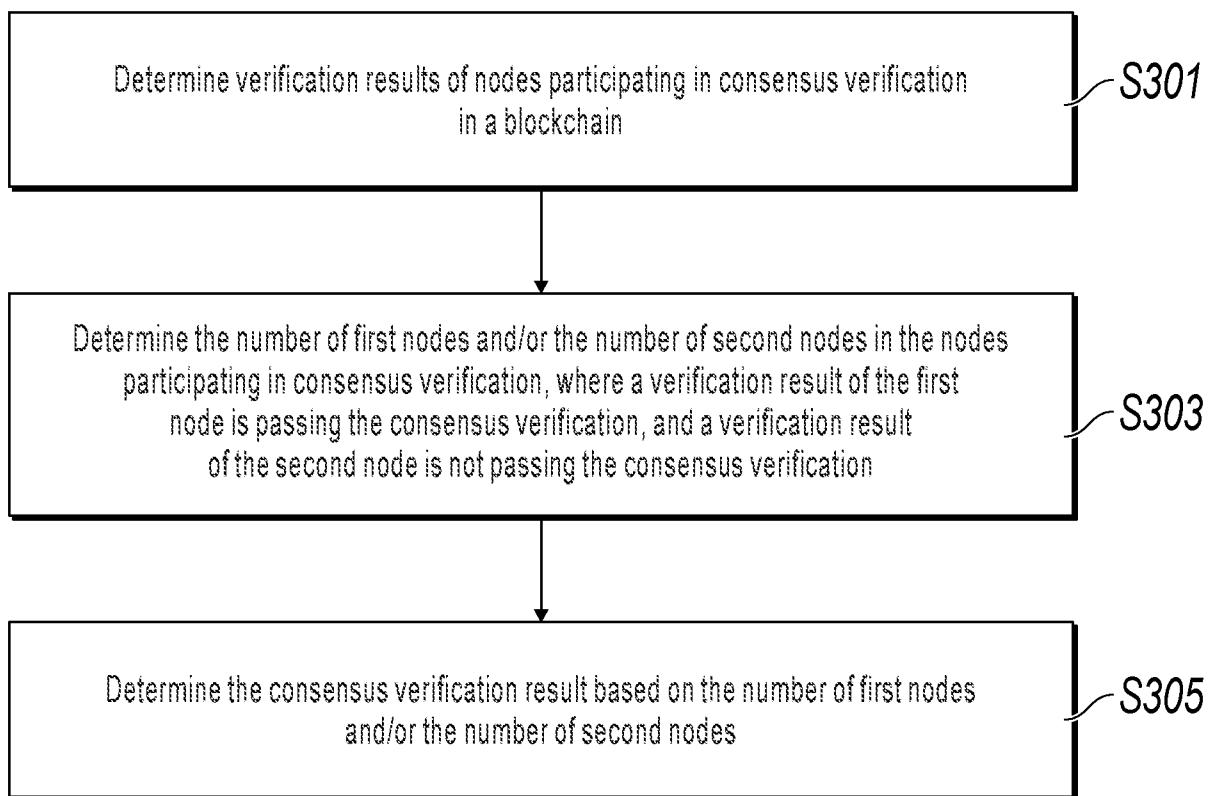
12. An apparatus for digital certificate management, the apparatus comprising a plurality of modules configured to perform the method according to any one of claims 1 to 11.

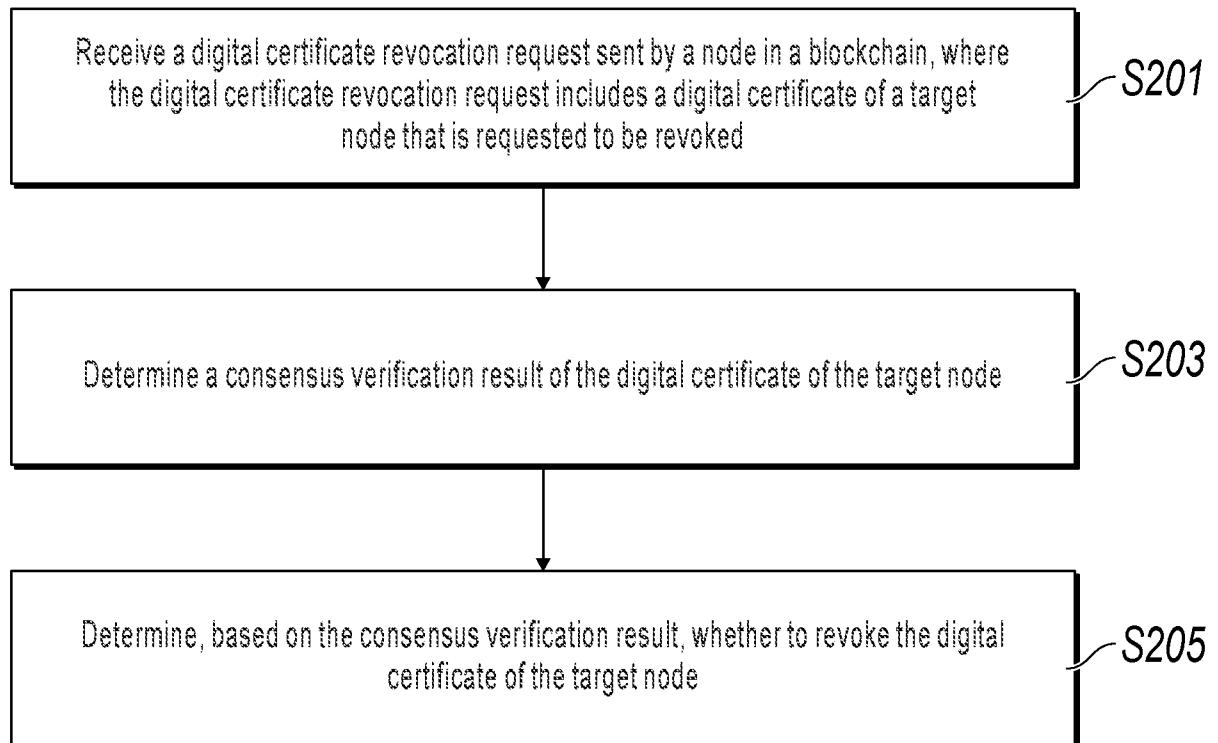
13. An electronic device, wherein the electronic device is applied to a blockchain and 20 comprises:

a processor; and

a storage, configured to store a computer executable instruction, wherein when the executable instruction is being executed, the processor performs the method according to any one of claims 1 to 11.

**FIG. 1**

**FIG. 2**

**FIG. 3**

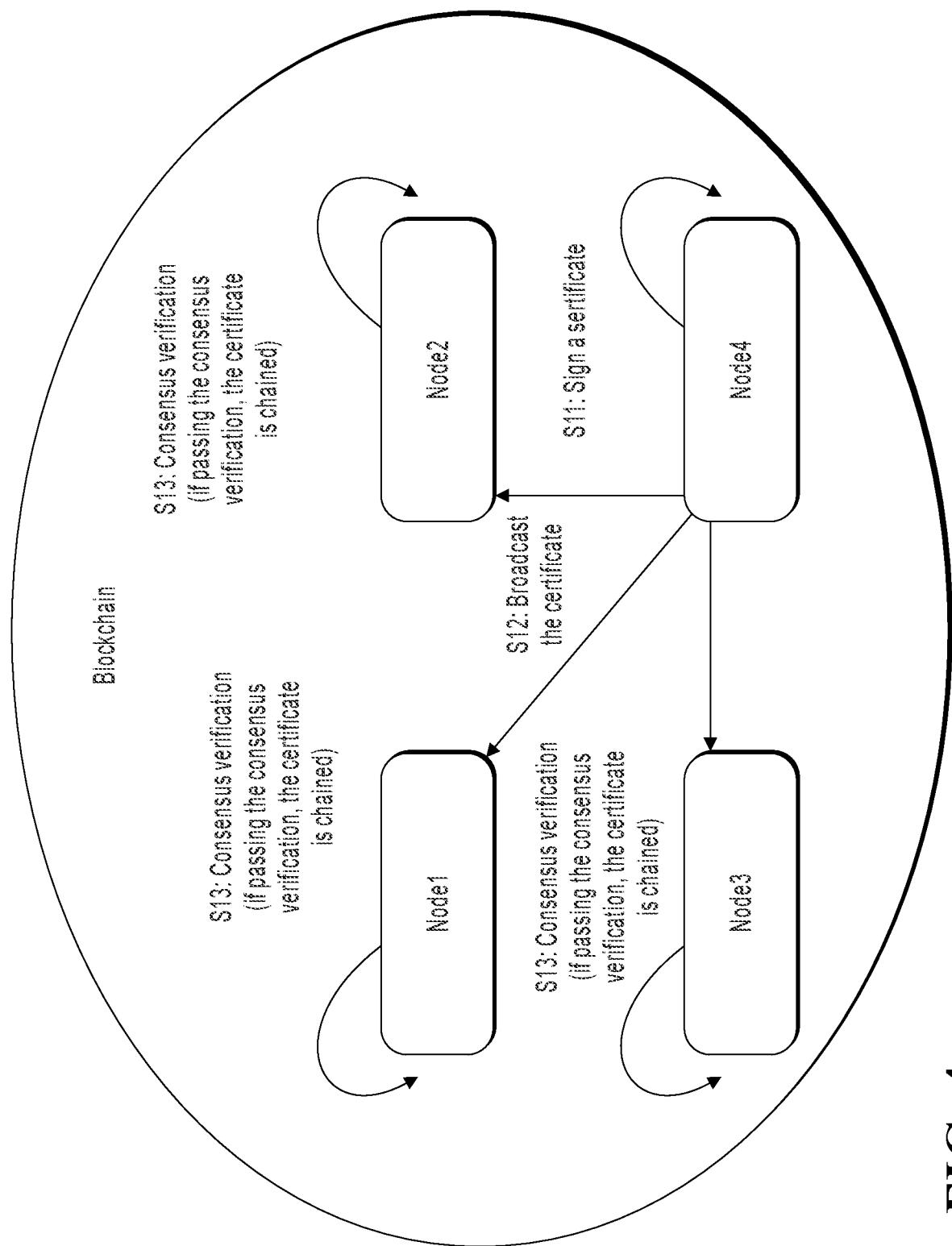
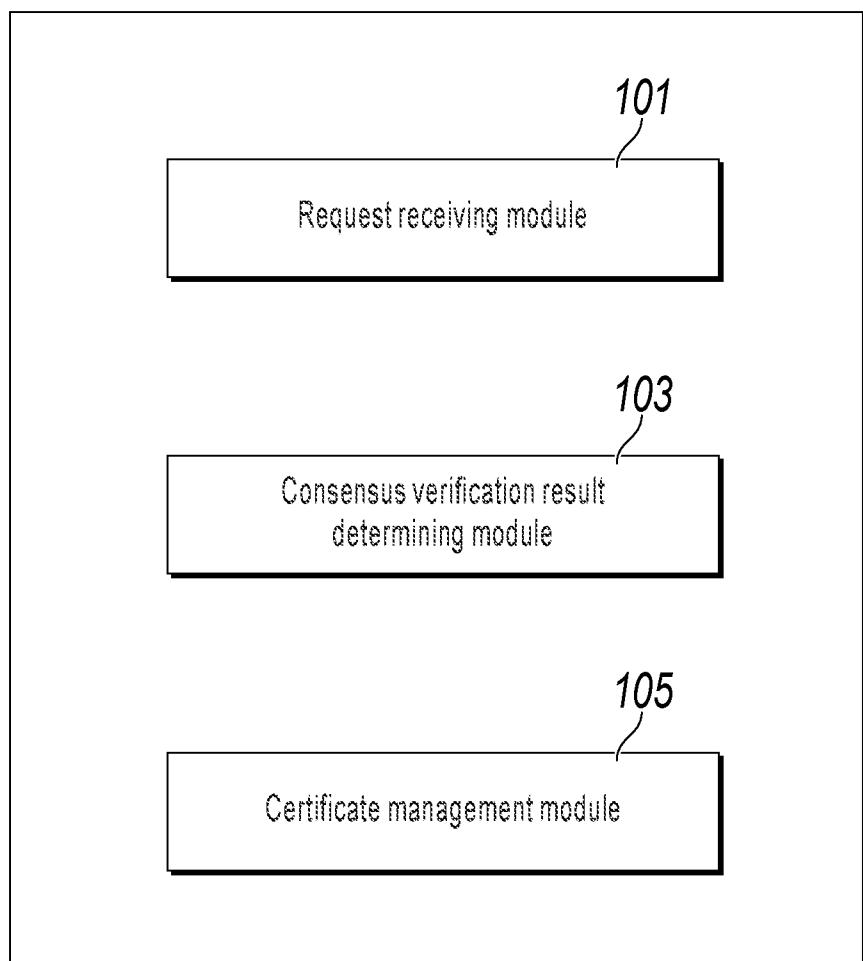
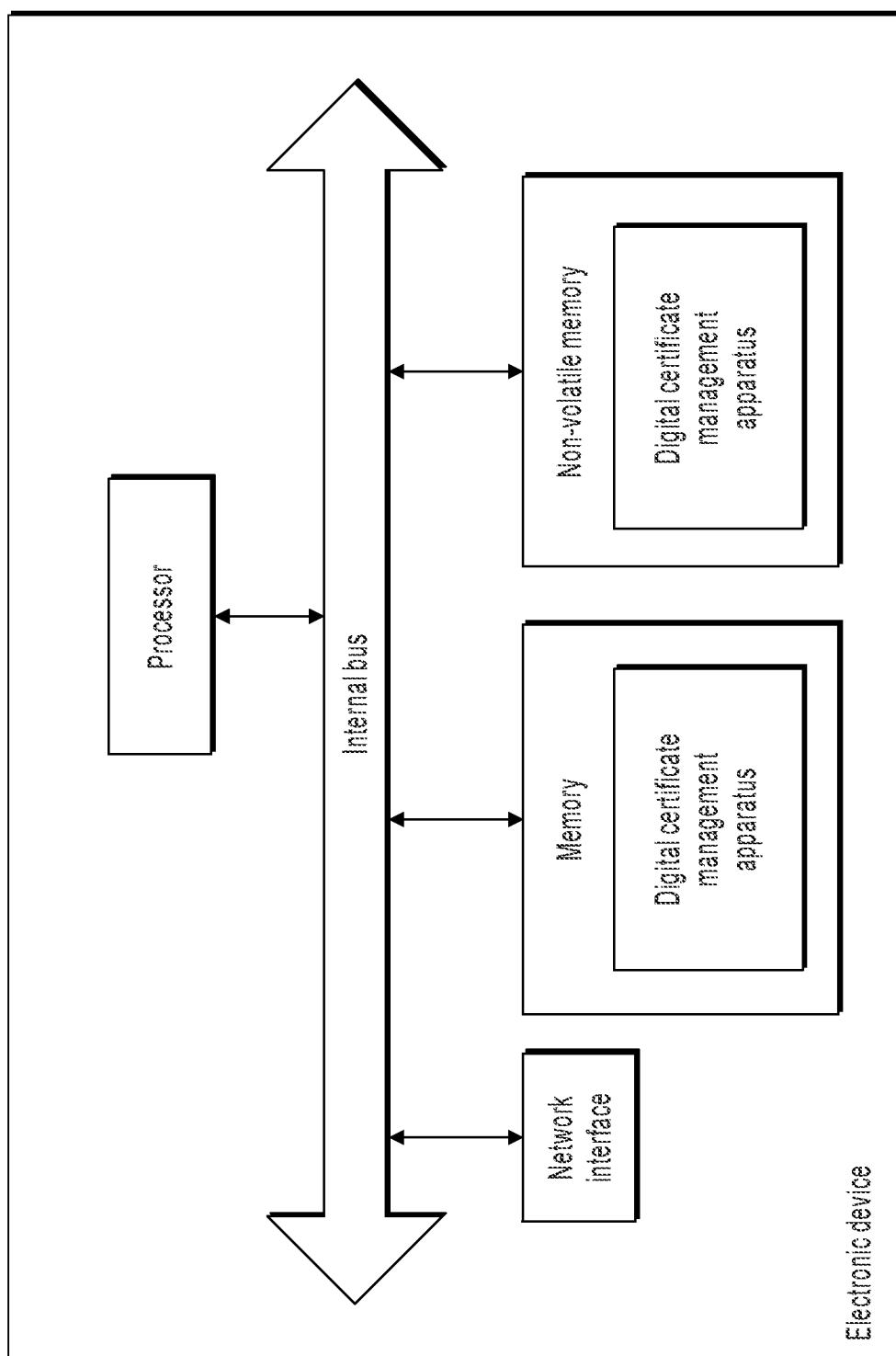
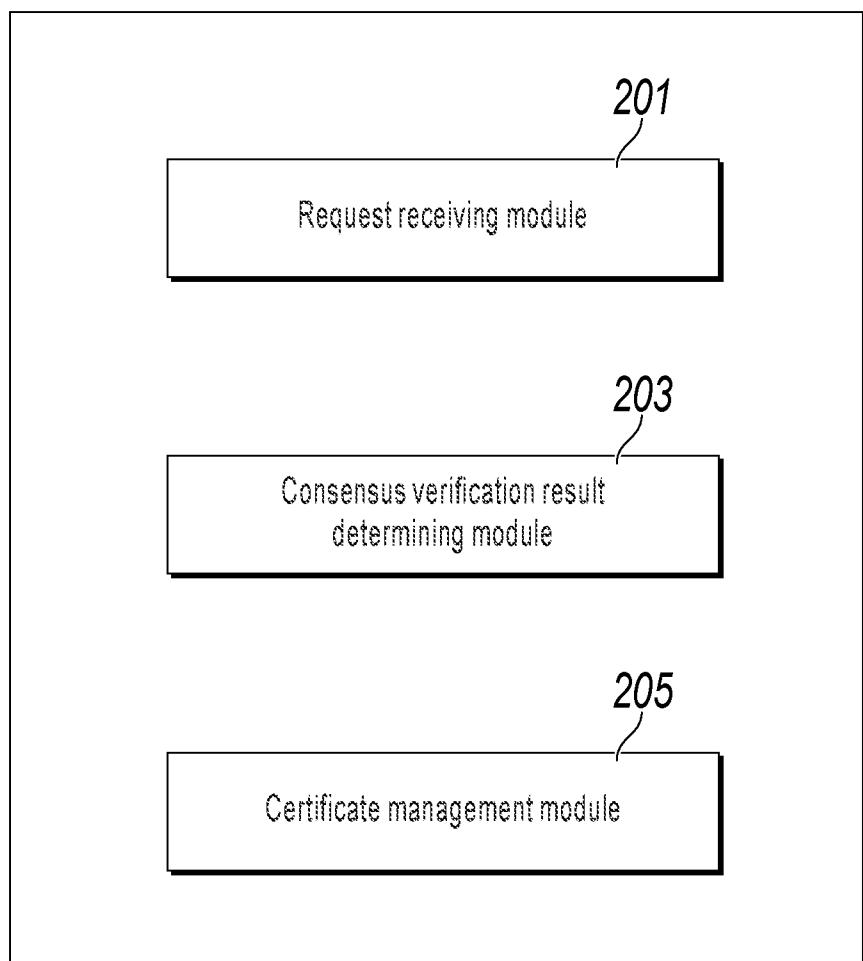
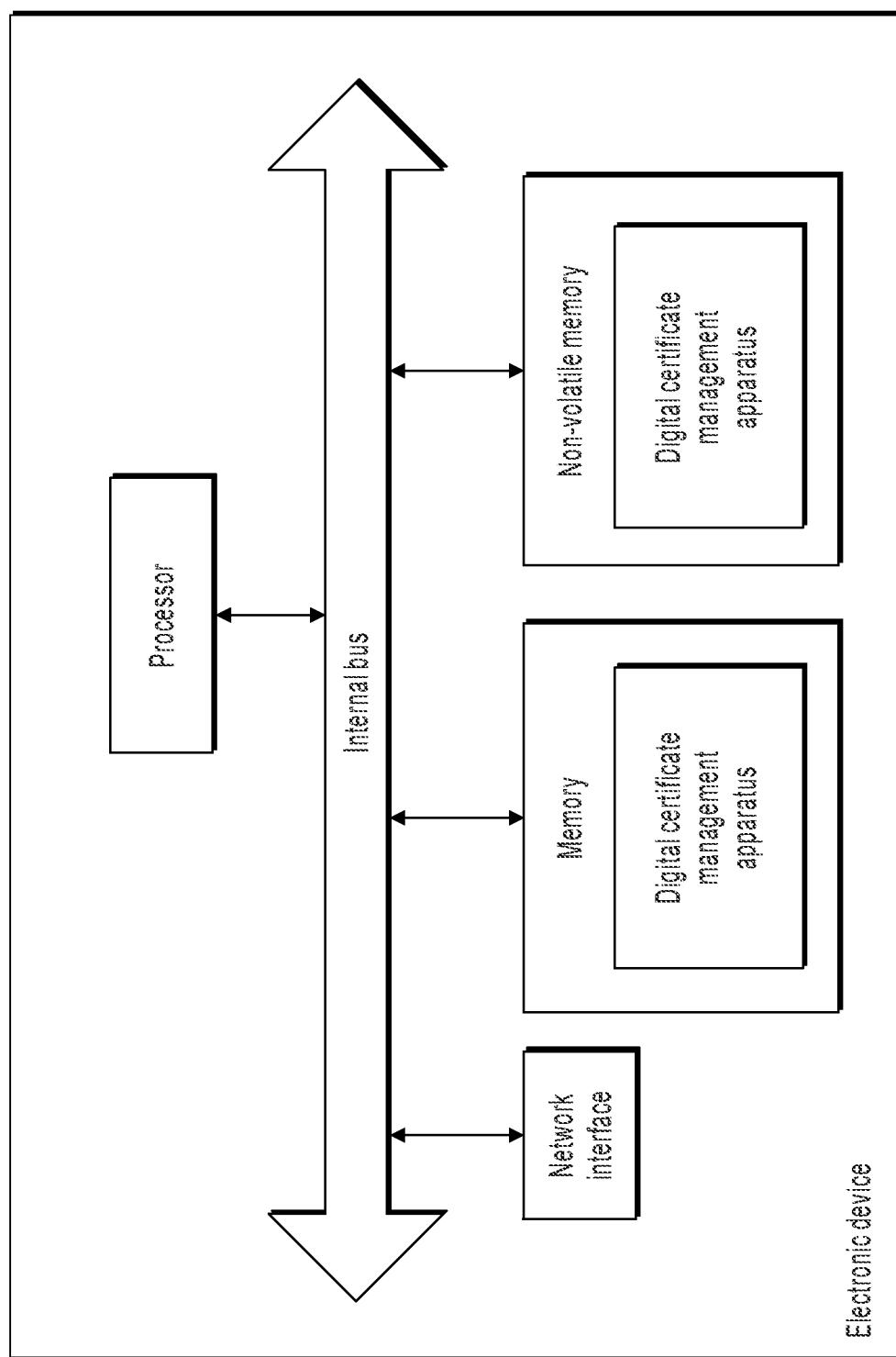


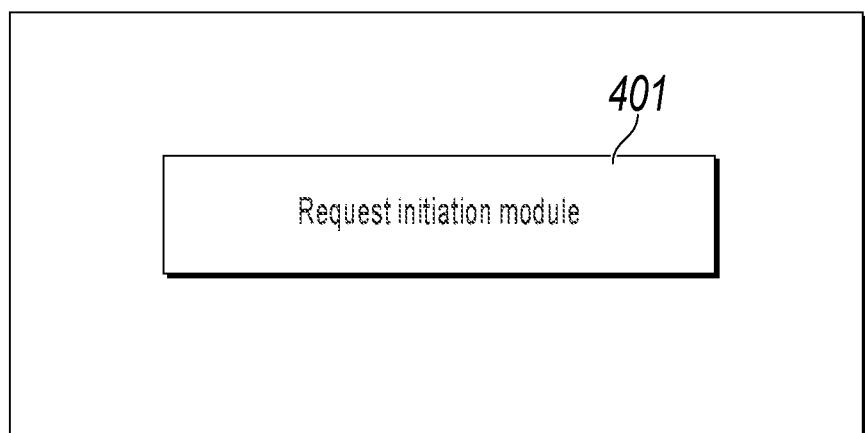
FIG. 4

**FIG. 5**

**FIG. 6**

**FIG. 7**

**FIG. 8**



**FIG. 9**

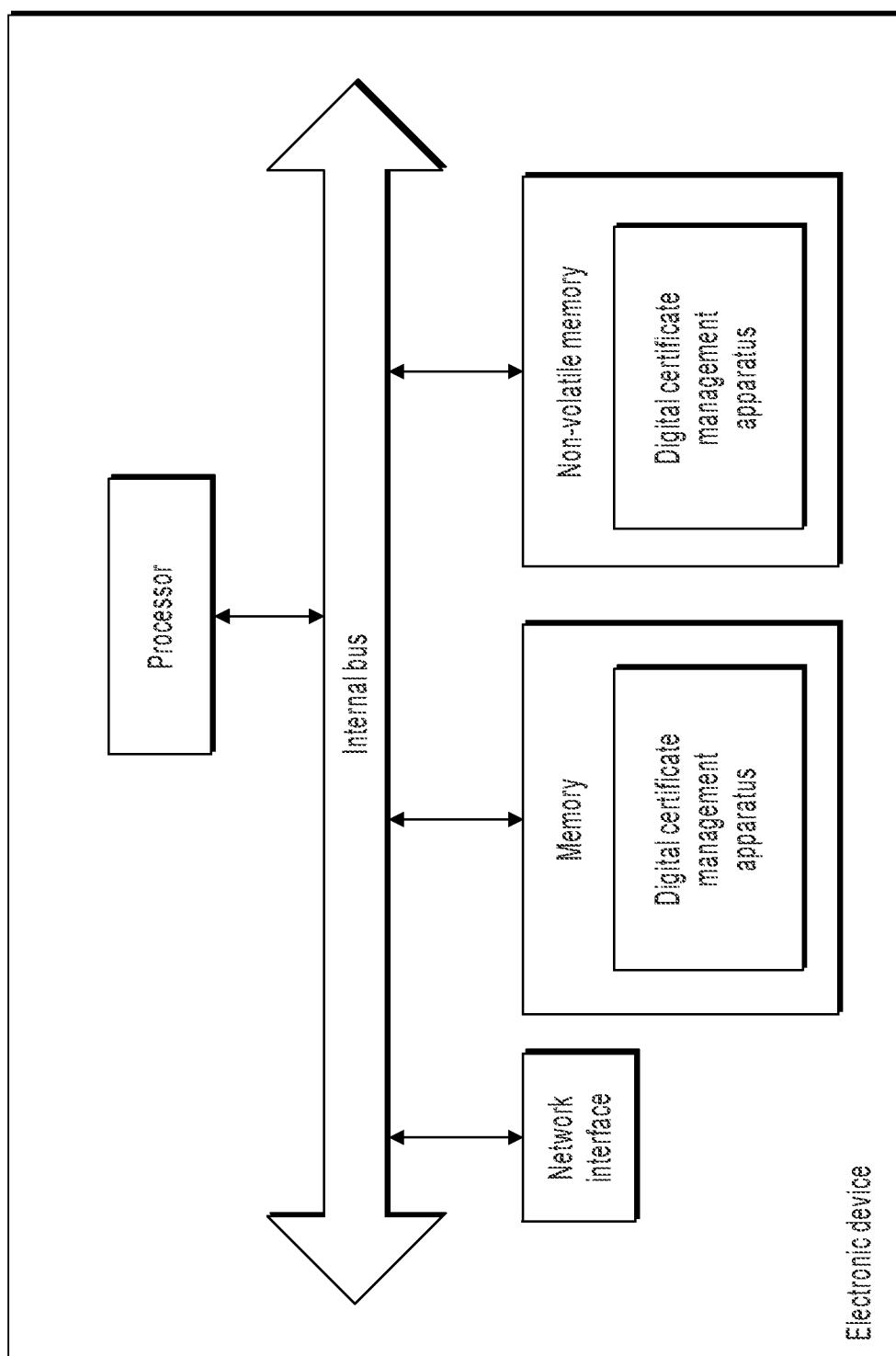
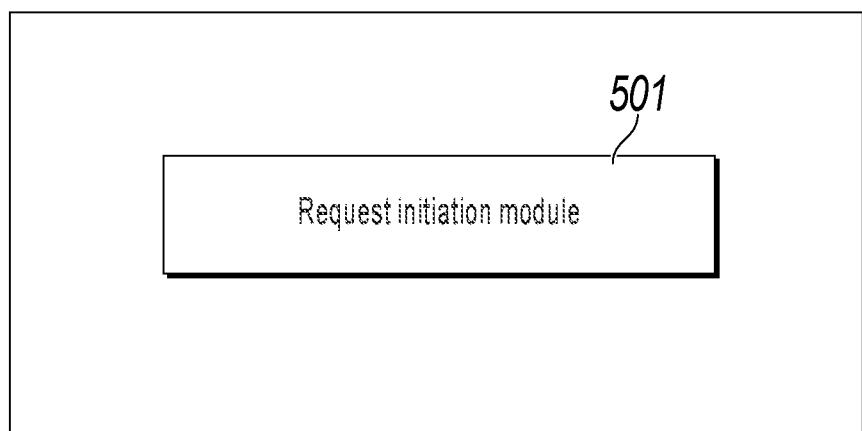
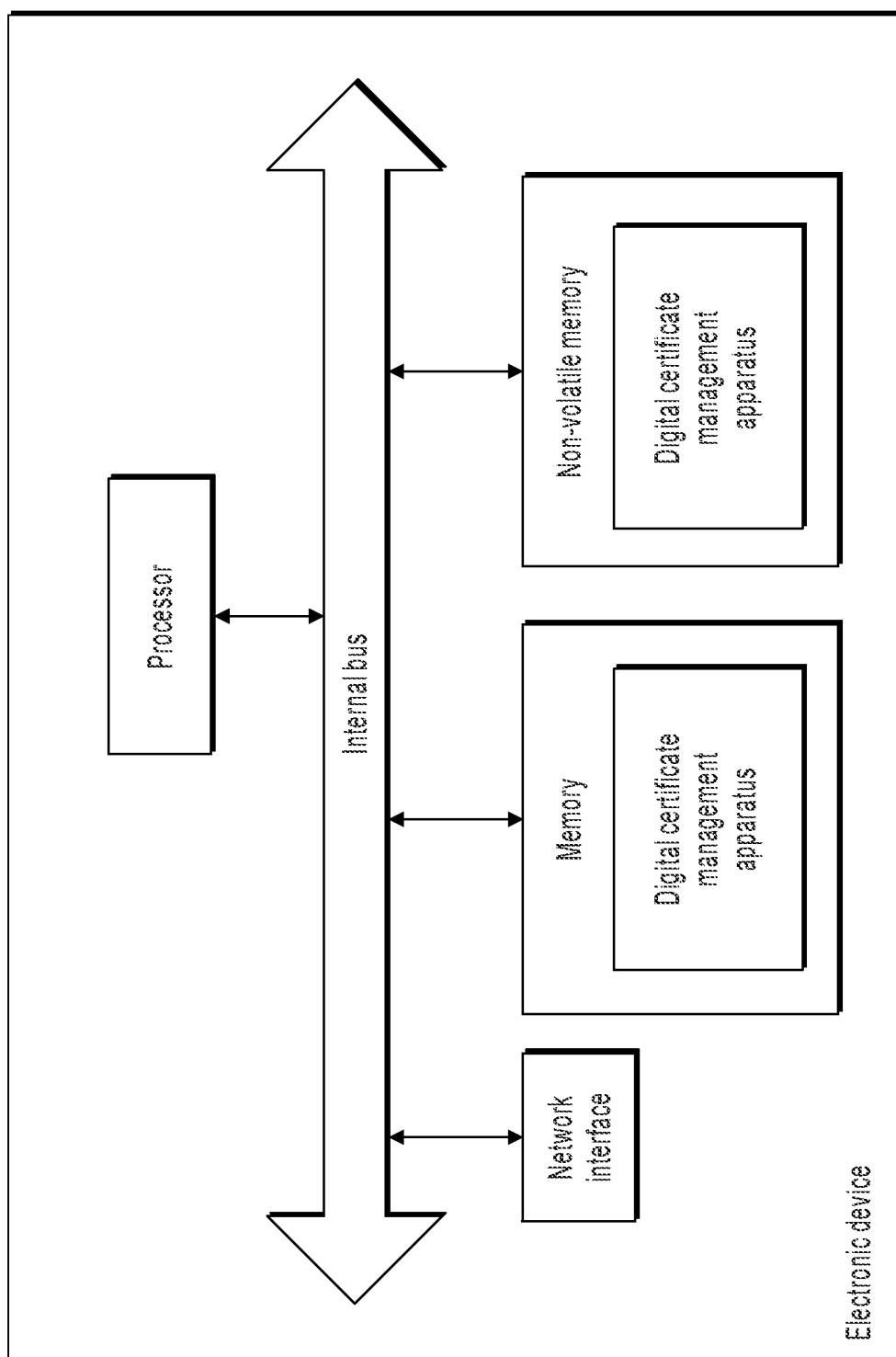


FIG. 10

**FIG. 11**



**FIG. 12**

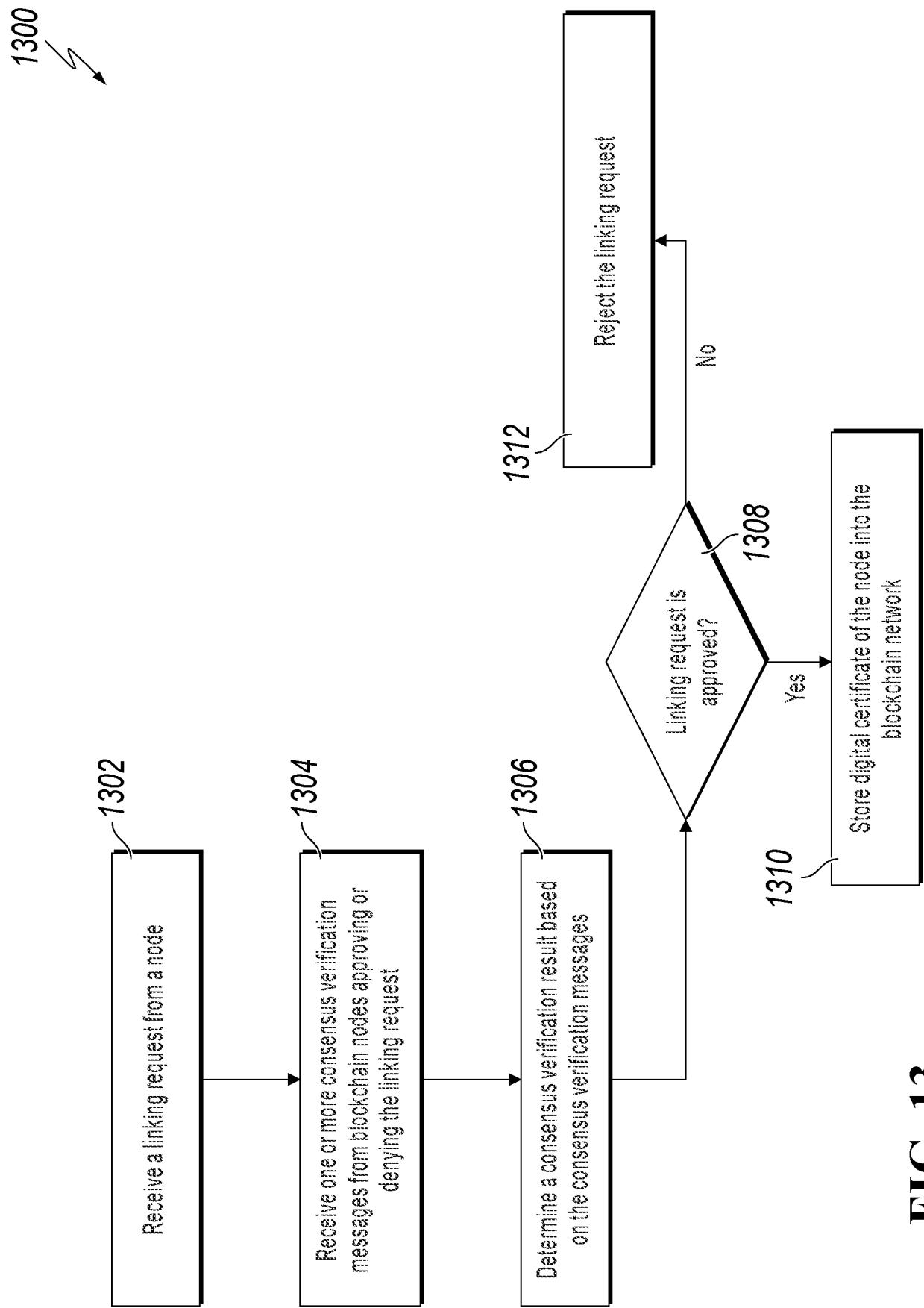


FIG. 13

# INTERNATIONAL SEARCH REPORT

International application No  
PCT/US2018/043901

A. CLASSIFICATION OF SUBJECT MATTER	INV. H04L29/06	G06Q20/38	G06Q20/40	H04L9/32	H04L29/08
ADD.					

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 9 635 000 B1 (MUFTIC SEAD [US]) 25 April 2017 (2017-04-25) abstract figures 1,4,6-12 column 1 column 3 - column 12 column 15 - column 16 -----	1,4,5, 7-13 2,3,6
X	Ietf: "RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", , 25 August 2015 (2015-08-25), XP055209498, Retrieved from the Internet: URL: <a href="https://tools.ietf.org/html/rfc5280">https://tools.ietf.org/html/rfc5280</a> [retrieved on 2015-08-25] page 1 - page 15 ----- -/-	5,7,9,10

Further documents are listed in the continuation of Box C.

See patent family annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
---	--

12 September 2018

20/09/2018

Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer
--	--------------------

Veshi, Erzim

**INTERNATIONAL SEARCH REPORT**

International application No PCT/US2018/043901
---

**C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Jae Kwon: "Tendermint: Consensus without Mining", , 19 March 2015 (2015-03-19), XP055493960, Retrieved from the Internet: URL: <a href="https://web.archive.org/web/20150319035333if_/http://tendermint.com:80/docs/tendermint.pdf">https://web.archive.org/web/20150319035333if_/http://tendermint.com:80/docs/tendermint.pdf</a> [retrieved on 2018-07-19] page 1 - page 8 -----	2,3,6
X	US 2015/356523 A1 (MADDEN WILLIAM EVAN [US]) 10 December 2015 (2015-12-10) paragraph [0029] - paragraph [0080] paragraph [0132] - paragraph [0144] -----	1-13

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No

PCT/US2018/043901

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 9635000	B1 25-04-2017	NONE	
US 2015356523	A1 10-12-2015	NONE	