

DEDICATED BLOCKCHAIN NODE DEVICES AND AUTOMATIC NODE ADDING METHODS AND APPARATUSES

TECHNICAL FIELD

[0001] The present disclosure relates to the field of terminal technologies, and in particular to dedicated blockchain node devices and automatic node adding methods and apparatuses thereof.

BACKGROUND

[0002] Blockchain technology (also called distributed ledger technology) is a decentralized distributed database technology having many characteristics of decentralization, openness, transparency, immutability and trustability and the like, and thus it is applicable to many application scenarios with high demands for data reliability.

SUMMARY

[0003] In view of this, one or more embodiments of the present disclosure provide dedicated blockchain node devices and automatic node adding methods and apparatuses thereof.

[0004] To achieve the above-mentioned object, one or more embodiments of the present disclosure provide the following technical solution:

[0005] According to a first aspect of one or more embodiments of the present disclosure, provided is an automatic node adding method of a dedicated blockchain node device, including:

[0006] receiving, by the dedicated blockchain node device, a configuration instruction after accessing a blockchain network, and configuring a first network address corresponding to a certificate authority center and a second network address corresponding to a first blockchain node in the blockchain network respectively according to the configuration instruction;

[0007] initiating, by the dedicated blockchain node device, an authentication request to the certificate authority center according to the first network address, and receiving a digital certificate returned by the certificate authority center after the certificate authority center determines the authentication request passes verification;

[0008] sending, by the dedicated blockchain node device, the digital certificate to the first blockchain node according to the second network address, wherein the digital certificate is used to trigger the first blockchain node to add the dedicated blockchain node device as a newly-added blockchain node in the blockchain network.

[0009] According to a second aspect of one or more embodiments of the present disclosure,

provided is an automatic node adding apparatus of a dedicated blockchain node device, including:

[0010] an address configuring unit, configured to enable the dedicated blockchain node device to receive a configuration instruction after accessing a blockchain network, and configure a first network address corresponding to a certificate authority center and a second network address corresponding to a first blockchain node in the blockchain network respectively according to the configuration instruction;

[0011] a certificate requesting unit, configured to enable the dedicated blockchain node device to initiate an authentication request to the certificate authority center according to the first network address, and receive a digital certificate returned by the certificate authority center after the certificate authority center determines the authentication request passes verification;

[0012] a certificate sending unit, configured to enable the dedicated blockchain node device to send the digital certificate to the first blockchain node according to the second network address, wherein the digital certificate is used to trigger the first blockchain node to add the dedicated blockchain node device as a newly-added blockchain node in the blockchain network.

[0013] According to a third aspect of one or more embodiments of the present disclosure, provided is a dedicated blockchain node device, including:

[0014] a processor;

[0015] a memory storing instructions executable by the processor;

[0016] wherein the processor implements the method according to the first aspect by running the executable instructions.

[0017] According to a fourth aspect of one or more embodiments of the present disclosure, provided is a computer readable storage medium for storing computer instructions, wherein the instructions are executed by a processor to implement steps of the method according to the first aspect.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] FIG. 1 is a flowchart of an automatic node adding method of a dedicated blockchain node device according to example embodiments of the present disclosure.

[0019] FIG. 2 is a schematic diagram of a scenario in which a dedicated blockchain node device realizes automatic node adding to a blockchain network according to example embodiments of the present disclosure.

[0020] FIG. 3 is an interaction flowchart in which a dedicated blockchain node device realizes automatic node adding according to example embodiments of the present disclosure.

[0021] FIG. 4 is a structural schematic diagram of a dedicated blockchain node device according to example embodiments of the present disclosure.

[0022] FIG. 5 is a block diagram of an automatic node adding apparatus of a dedicated blockchain node device according to example embodiments of the present disclosure.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0023] Example embodiments will be described in detail herein with the example embodiments thereof expressed in the drawings. When the following descriptions involve the drawings, same numbers in different drawings represent same or similar elements unless stated otherwise. The implementations described in the following example embodiments do not represent all implementations consistent with one or more embodiments of the present disclosure. On the contrary, they are merely embodiments of apparatuses and methods consistent with some aspects of one or more embodiments of the present disclosure described in detail in the appended claims.

[0024] It should be noted that the steps of corresponding method is not necessarily performed according to the sequence shown in the present disclosure in other embodiments. In some other embodiments, the steps included in the corresponding method can be more or less than described in the present disclosure. Further, a single step described in the present disclosure can be divided into several steps for descriptions in other embodiments while several steps described in the present disclosure can be combined into a single step for descriptions in other embodiments.

[0025] In the early stage of development of the blockchain technology, users mostly add their own personal computer (PC) and laptop computer and the like into a blockchain network to become a blockchain node in the blockchain network. At this time, the stage can be called 1.0 architecture era of blockchain network, in which the behaviors of users to participate in the blockchain network are autonomous and the users also need to perform autonomous maintenance, for example, perform maintenance and configuration and so on for their devices (for example, PC) participating in the blockchain network. Along with continuous development of the blockchain technology, especially along with increasing needs of users for infrastructures with high performance and high availability, the blockchain network develops into 2.0 architecture era based on cloud service. In the 2.0 architecture era, Blockchain-as-a-Service (BaaS) provides fast and convenient solutions for fast blockchain

deployment and technical implementation and supports a large number of blockchain service projects. Generally, BaaS is built on infrastructures such as public cloud or private cloud, which introduces heavy dependence on infrastructure as well as providing strong deployment capability. However, because blockchain is a typical distributed computing technology, not all nodes can be migrated to clouds but privatization deployment is needed. The additional technical migration and maintenance costs brought by the privatization deployment cause inconsistent technical interfaces and high deployment and maintenance costs during an actual implementation. Therefore, to satisfy the needs of users for privatization and security and the like of the blockchain network, architecture needs to be further upgraded to the blockchain network, thereby realizing 3.0 architecture era based on dedicated blockchain node device (blockchain all-in-one machine).

[0026] Software and hardware integration can be realized for the dedicated blockchain node device. When providing a dedicated blockchain node device, a provider will not only provide hardware devices of the dedicated blockchain node device to users but also provide software configurations for realizing deep optimizations of the hardware devices integrated into the dedicated blockchain node device, thereby realizing the above-mentioned software-hardware integration.

[0027] Hardware optimization can be realized for the dedicated blockchain node device. For example, a dedicated smart contract processing chip can be deployed on the dedicated blockchain node device. For example embodiments, the smart contract processing chip can be Field Programmable Gate Array (FPGA) chip, or another type of chip to increase the processing efficiency for a smart contract. A hardware root-of-trust key can be deployed on the smart contract processing chip, for example, the hardware root-of-trust key can be pre-programmed by the provider into the smart contract processing chip and the provider can also know a public key corresponding to the hardware root-of-trust key (for example, the key is disclosed). Therefore, the smart contract processing chip can send negotiation information to the provider and sign the negotiation information by using the hardware root-of-trust key, so that the provider can verify the signature based on the corresponding public key; and, after successful signature verification, it is ensured that the smart contract processing chip and the provider obtain the same key through negotiation based on the above-mentioned negotiation information. The negotiated key can include a file deployment key, and thus the provider can encrypt and transmit a binary image file needed by the blockchain node to the smart contract processing chip based on the file deployment key, and the smart contract processing chip can decrypt and deploy the binary image file based on the file deployment key. The negotiated key can include a service secret deployment key, and thus the provider can encrypt and

transmit a node private key of the blockchain node, a service root key of the blockchain node etc., to the smart contract processing chip based on the service secret deployment key, and the smart contract processing chip can obtain and deploy the node private key and the service root key and the like based on the service secret deployment key to satisfy the privacy transaction needs in a blockchain scenario. For example, the node private key corresponds to a node public key, and thus a client device can perform encrypted transmission for a blockchain transaction by using the node public key, and the blockchain node can perform decryption by using the node private key. The service root key is a symmetric key which can be used to perform encrypted storage for service data such as contract codes and values of contract status and the like. The service root key may not be directly used, and the smart contract processing chip can perform encryption and decryption by using a derivation key of the service root key to reduce the security risk of the service root key. Through reliable management for the node private key and the service root key (or its derivation key), data will be always in encrypted state unless processed by the smart contract processing chip. Therefore, the smart contract processing chip actually forms a Trusted Execution Environment (TEE) of hardware on the dedicated blockchain node device, so as to ensure the data requiring privacy protection such as transactions, contract codes, and contract statuses will not be leaked.

[0028] For another example, an intelligent network card can be deployed on the dedicated blockchain node device. In addition to realizing a traditional network card function, the intelligent network card also can replace or assist a CPU of the dedicated blockchain node device to perform partial functions so as to offload computation of the CPU. Especially, the operations with intensive network I/O can be transferred from CPU to the intelligent network card to perform, so that the CPU can process more computation-intensive operations, for example embodiments, transaction processing, and storage processing and the like. Compared with other components (for example, CPU) on the dedicated blockchain node device, the intelligent network card is closer to the network regardless of physical level or logical level, so the intelligent network card can always fetch data transmitted in the network preferentially. Therefore, with no storage access or a small amount of storage access is involved, the intelligent network card can process these data with a relatively higher processing efficiency and a relatively smaller delay, and a relatively larger throughput, so as to achieve a higher performance benefit with a lower cost. For example embodiments, in consensus algorithm, there is almost no need to access storage except in the cases of change of network status, addition and deletion of node, change of consensus configuration and the like. Therefore, the consensus operation can be completed by the intelligent network card and only need to inform the CPU of a consensus result. Therefore, the CPU is not needed to directly participate in the

consensus process, thereby significantly improving the consensus efficiency. Similarly, the same effect can be achieved in forwarding transactions by the intelligent network card and achieving block synchronization by the intelligent network card on a newly-added blockchain node and the like and will not be repeated herein. Furthermore, after receiving transactions, the intelligent network card can identify or filter out a replay transaction by comparing with the received transaction with historical transactions, for example, compare data fields of sender information of transaction, destination address, time stamp, and hash value and the like. The intelligent network card can also perform content analysis for those received transactions, so as to filter out illegal transactions or predefined undesired transactions and the like as a supplementation to layer-2 or layer-3 packet filtering implemented by a switch.

[0029] For another example, a cryptographic acceleration card which is also called a high speed cryptographic card can be deployed on the dedicated blockchain node device. The cryptographic acceleration card can realize total encrypted memory, defend against side-channel attacks by hardware reinforcement, and also realize physical protection against approaches such as probe, laser and the like, having very high security. For example, the cryptographic acceleration card used on the dedicated blockchain node device can have level-2 qualification from the State Cryptography Administration, level-3 qualification from the State Cryptography Administration and the like. When the cryptographic acceleration card is deployed, the hardware roof-of-trust key as described above can be maintained in the cryptographic acceleration card, and the cryptographic acceleration card can perform signature operation based on the hardware roof-of-trust key and replace or assist the smart contract processing chip to complete the operations such as the key negotiation as described above. Similarly, the cryptographic acceleration card can be used to maintain a public key so that the cryptographic acceleration card can realize signature verification operation based on the maintained public key. In short, at least part of operations relating to key management, encryption and decryption, and signature verification and the like on the dedicated blockchain node device can be handed over to the cryptographic acceleration card, so that very high security can be realized and task offloading can be realized for the CPU of the dedicated blockchain node device or the above-mentioned smart contract processing chip, thereby improving the processing efficiency.

[0030] Software optimization can be realized for the dedicated blockchain node device. For example, a certificate authority service can be built in the dedicated blockchain node device to realize automatic certificate issuing, node identity authentication, automatic blockchain construction, and automatic adding of blockchain node, thereby realizing the plug and play of the dedicated blockchain node device. In this case, a user can realize fast deployment of the

dedicated blockchain node device. In addition to quickly establishing a private blockchain network among a plurality of dedicated blockchain node devices, the dedicated blockchain node device can integrate a standardized on-cloud service interface to enable the dedicated blockchain node device to automatically connect to on-cloud service, thereby realizing hybrid deployment between the dedicated blockchain node device and the cloud-deployed blockchain node and to construct a hybrid blockchain network. The dedicated blockchain node device can also integrate a standardized cross-chain service interface to enable the dedicated blockchain node device to realize cross-chain services based on a standardized cross-chain protocol or standardized cross-chain service, thereby greatly expanding the application scenarios of the dedicated blockchain node device, and satisfying the cross-chain needs of users. For example, cross-chain data interaction between different blockchain networks is achieved, and for another example, cross-chain data interaction between the blockchain network and an off-chain computing node and the like is achieved (for example, the off-chain computing node shares computation task for the blockchain node and the like).

[0031] Based on a unified software logic adopted on each dedicated blockchain node device, the dedicated blockchain node device in the present disclosure can realize automatic node adding after accessing a blockchain network, which will be described below in combination with the accompanying drawings.

[0032] FIG. 1 is a flowchart of an automatic node adding method of a dedicated blockchain node device according to example embodiments of the present disclosure. As shown in FIG. 1, the method can include the following steps.

[0033] At step 102, the dedicated blockchain node device receives a configuration instruction after accessing a blockchain network, and configures a first network address corresponding to a certificate authority center and a second network address corresponding to a first blockchain node in the blockchain network respectively according to the configuration instruction.

[0034] After accessing the blockchain network, the dedicated blockchain node device only realizes hardware-level network access. Logically, the dedicated blockchain node device has not become a blockchain node in the blockchain network. The dedicated blockchain node device needs to adopt the technical solution of the present disclosure to become a blockchain node in the blockchain network.

[0035] The configuration instruction received by the dedicated blockchain node device is used to configure the first network address and the second network address as described above. The configuration instruction can be input into the dedicated blockchain node device by a user using a peripheral device, that is, the values of the first network address and the

second network address are actually configured by the user; or the first network address and the second network address are pre-configured in the dedicated blockchain node device upon leaving factory and in this case, the configuration instruction can be generated automatically by the dedicated blockchain node device after initial startup.

[0036] The first network address and the second network address can be IP addresses. The first network address and the second network address can be different. At this time, the certificate authority center and the first blockchain node are different entities. The certificate authority center can be an independent device different from a blockchain node in the blockchain network so as to be specially used to issue a certificate, or the certificate authority center can be deployed at another blockchain node different from the first blockchain node in the blockchain network.

[0037] In some cases, the first network address and the second network address can be identical. At this time, the certificate authority center and the first blockchain node are the same one entity, for example, assuming that the first blockchain node initiates a certificate authority (CA) service. Because the first network address and the second network address are identical, it is equivalent to configuring only one network address. The first blockchain node can be formed by the dedicated blockchain node devices, or the first blockchain node can be another type of node device, which is not limited herein.

[0038] Actually, each blockchain node in the blockchain network can be in-built with a CA service. But, in general, only some of the blockchain nodes in the network will initiate the CA service, and typically, only one blockchain node initiates the CA service and other blockchain nodes need to apply for a certificate to the dedicated blockchain node device. Of course, there can be differences between different blockchain nodes, for example, the CA service is built in only some of the blockchain nodes in the network. In this case, one or more of these blockchain nodes can initiate the CA service and assist in issuing a certificate to other blockchain nodes without built-in CA service.

[0039] At step 104, the dedicated blockchain node device initiates an authentication request to the certificate authority center based on the first network address, and receives a digital certificate returned by the certificate authority center after the certificate authority center determines the authentication request passes verification.

[0040] The blockchain network can be a dedicated network. The dedicated blockchain node device accesses the dedicated network via a tunnel to perform operations such as applying for digital certificate and participating in blockchain network and the like. Because the dedicated blockchain node device is needed to provide corresponding network information and login authentication information and the like when establishing the tunnel, a corresponding rule is

set for accessing the dedicated blockchain node device, which is equivalent to realizing permission control for accessing the dedicated blockchain node device, thereby avoiding unauthorized access into the blockchain network. The certificate authority center can be deployed in the blockchain network or in a public network outside the blockchain network, as long as the dedicated blockchain node device can smoothly access. If the certificate authority center is deployed in the blockchain network, the certificate authority center can be a blockchain node already initiated a CA service in the blockchain network as above-mentioned. Of course, the certificate authority center can also be an independent device. If the certificate authority center is deployed in a public network outside the blockchain network, the certificate authority center can be deployed on the BaaS platform in the public network.

[0041] Based on different network environments where the certificate authority center is located, the processes in which the dedicated blockchain node device initiates an authentication request according to the first network address may be different to some extent, but the authentication request will be eventually sent to the certificate authority center. When issuing a digital certificate, the certificate authority center needs to use its own CA identity key, where the CA identity key includes a CA identity private key and a CA identity public key. Similarly, the dedicated blockchain node device also has an identity key of a dedicated node device which includes a private key of a dedicated node device and a public key of a dedicated node device. The private key of the dedicated node device is maintained by the dedicated blockchain node device, and the public key of the dedicated node device is included in the above-mentioned authentication request. Further, the authentication request includes other description information of the dedicated blockchain node device. These description information are used for the certificate authority center to determine the identity of the dedicated blockchain node device. After determining the authentication request passes verification, the certificate authority center signs the public key of the dedicated node device, the description information of the dedicated node device, and information of the certificate authority center by using the above-mentioned CA private key, so as to generate the digital certificate of the dedicated blockchain node device.

[0042] At step 106, the dedicated blockchain node device sends the digital certificate to the first blockchain node according to the second network address, wherein the digital certificate is used to trigger the first blockchain node to add the dedicated blockchain node device as a newly-added blockchain node in the blockchain network.

[0043] The digital certificate issued by the certificate authority center is used to indicate that the dedicated blockchain node device corresponding to the digital certificate already passes the identity authentication of the certificate authority center. Therefore, by performing

verification for the digital certificate provided by the dedicated blockchain node device, the first blockchain node can add the dedicated blockchain node device as a newly-added blockchain node in the blockchain network after successful verification.

[0044] When performing verification for the digital certificate of the dedicated blockchain node device, the first blockchain node needs to use a root certificate. The root certificate is a digital certificate issued by the certificate authority center for itself. The certificate authority center generates the above-mentioned root certificate by signing the CA public key and description information of the certificate authority center by using the above-mentioned CA private key. Because the certificate authority center generates the digital certificate by signing its own public key with its own private key, the digital certificate corresponding to the certificate authority center is a root certificate which is also called a self-signed certificate. The first blockchain node can obtain the CA public key included in the root certificate and perform signature verification for the digital certificate sent by the dedicated blockchain node device by using the CA public key after receiving the digital certificate. In this way, in a case of successful verification, the first blockchain node determines the digital certificate is issued by the certificate authority center and accepts the corresponding dedicated blockchain node device as a blockchain node in the blockchain network.

[0045] After being determined as passing verification by any blockchain node in the blockchain network, the digital certificate is used to indicate the any blockchain node to initiate a transaction for adding node in the blockchain network. The transaction is executed after all blockchain nodes in the blockchain network pass a consensus, so that the dedicated blockchain node device corresponding to the digital certificate is added as a newly-added blockchain node in the blockchain network.

[0046] Take the first blockchain node as an example, the first blockchain node verifies the digital certificate sent by the dedicated blockchain node device by using the CA public key included in the root certificate, and creates a transaction for adding node after successful verification. For example, the type of the transaction is a node adding type (for example, the type can be determined according to the value of Type field of transaction), and the Data field of the transaction includes information of the above-mentioned dedicated blockchain node device. The transaction is sent by the first blockchain node to all blockchain nodes in the blockchain network and a consensus is performed among all blockchain nodes: if the above-mentioned transaction passes the consensus, it indicates that all blockchain nodes in the blockchain network accept the above-mentioned dedicated blockchain node device. In this case, the above-mentioned transaction is recorded into a blockchain, and the dedicated blockchain node device is added as a newly-added blockchain node in the blockchain network.

Further, each blockchain node in the blockchain network can maintain one node information list which is used to record information of a blockchain node accepted by the each blockchain node, for example, the information can include IP address and public key and the like. Thus, after the above-mentioned dedicated blockchain node device is accepted, the information of the dedicated blockchain node device is recorded by each blockchain node in the blockchain network into the node information list maintained by each blockchain node. Similarly, after the dedicated blockchain node device becomes a newly-added blockchain node, the dedicated blockchain node device can synchronize the node information list in addition to synchronizing blockchain data and status data and the like with the existing blockchain nodes.

[0047] After the dedicated blockchain node device accesses the blockchain network, a blockchain node in the blockchain network can automatically discover the dedicated blockchain node device. For example, when a second blockchain node discovers the dedicated blockchain node device, the second blockchain node can proactively send inquiry information to the dedicated blockchain node device. Correspondingly, the dedicated blockchain node device can send the above-mentioned digital certificate to the second blockchain node in response to receiving the inquiry information, where the digital certificate is used to trigger the second blockchain node to add the dedicated blockchain node device as a newly-added blockchain node in the blockchain network. The process in which the second blockchain node adds the dedicated blockchain node device as a newly-added blockchain node is similar to that of the first blockchain node, that is, a transaction for adding node is initiated after it is determined the digital certificate passes verification, so that the dedicated blockchain node device is added as a newly-added blockchain node after the transaction passes consensus, which will not be repeated herein. Although the dedicated blockchain node device can proactively send the digital certificate to the first blockchain node for identity verification according to a configured second network address, the first blockchain node may not work normally due to some reason and thus cannot smoothly add the dedicated blockchain node device as a newly-added blockchain node. In this case, with the automatic discovery function of the second blockchain node for the dedicated blockchain node device, it can be ensured that the dedicated blockchain node device can be smoothly added to the blockchain network without configuring a new second network address in a case of abnormality of the first blockchain node, thus avoiding failure of adding the dedicated blockchain node device. In this way, a time needed for adding the dedicated blockchain node device can be shortened.

[0048] FIG. 2 shows an example scenario where a dedicated blockchain node device realizes automatic node adding in a blockchain network. FIG. 2 involves four dedicated blockchain node devices, i.e. a dedicated blockchain node device 21, a dedicated blockchain node device

22, a dedicated blockchain node device 23, and a dedicated blockchain node device 24. Of course, the quantity of the dedicated blockchain node devices is not limited herein. Assuming that the dedicated blockchain node devices 22-24 already become blockchain nodes in the blockchain network, the dedicated blockchain node device 21 can desire to participate in the blockchain network as a newly-added node and become a new node of the blockchain network through the interaction process of FIG. 3.

[0049] At step 301, the dedicated blockchain node device 21 configures an IP address.

[0050] The dedicated blockchain node device 21 configures an IP address of the CA center and an IP address of the original blockchain node respectively according to a received IP address configuration instruction. For example, the IP address of the CA center actually is an IP address of the dedicated blockchain node device 22, and the IP address of the original blockchain node actually is an IP address of the dedicated blockchain node device 23.

[0051] Herein, the dedicated blockchain node device 22, on the one hand, is configured as a blockchain node and on the other hand, initiates the CA service, such that the dedicated blockchain node device 22 is also configured as the above-mentioned CA center. Of course, in other embodiments, the blockchain node and the CA center are not necessarily configured in a same device, which is not limited herein. The IP address of the original blockchain node can also be an IP address of any blockchain node, for example, the dedicated blockchain node device 22 and the dedicated blockchain node device 24 and the like in the blockchain network in addition to the IP address of the dedicated blockchain node device 23.

[0052] At step 302, the dedicated blockchain node device 21 generates and sends an authentication request to the dedicated blockchain node device 22.

[0053] The dedicated blockchain node device 21 generates an identity key of a dedicated node device which can include a private key of a dedicated node device and a public key of a dedicated node device. The authentication request generated by the dedicated blockchain node device 21 can include the public key of the dedicated node device and description information of the dedicated blockchain node device 21. The description information of dedicated blockchain node device can include ID information, product serial number, IP address, MAC address and the like. Thus, the description information is not limited herein as long as it can prove the identity of the dedicated blockchain node device.

[0054] At step 303, the dedicated blockchain node device 22 performs identity verification and generates and returns a digital certificate to the dedicated blockchain node device 21.

[0055] After receiving the authentication request from the dedicated blockchain node device 21, the dedicated blockchain node device 22 verifies the description information of the dedicated blockchain node device 21 included in the authentication request through the CA

service and then generates the digital certificate for the dedicated blockchain node device 21 after successful verification. Specifically, there is a CA identity key in the dedicated blockchain node device 22, and the CA identity key includes a CA private key and a CA public key. The CA service can sign the public key of the dedicated node device and the description information of the dedicated blockchain node device 22, and the description information of the dedicated blockchain node device 21 as described above by using the CA private key to generate a digital certificate corresponding to the dedicated blockchain node device 21. Herein, the description information of the dedicated blockchain node device 21 adopted for signature may be inconsistent with the description information of the dedicated blockchain node device 22, for example, they can include different types of description information, which depends on a rule set by the CA service. Similarly, the description information of the dedicated blockchain node device 21 included in the authentication request can be inconsistent with the description information of the dedicated blockchain node device 21 adopted for signature, for example, the description information adopted for signature can be only part of the description information included in the authentication request, and especially can exclude part of description information that is not suitable for disclosure (for example, relating to privacy), for another example, the description information adopted for signature can be a hash value of the description formation included in the authentication request. Thus, the digital certificate can fully correspond to the description information included in the authentication request, and be prevented from disclosing the description information unsuitable for disclosure.

[0056] At step 304, the dedicated blockchain node device 21 sends the digital certificate to the dedicated blockchain node device 23 for verification.

[0057] At step 305, the dedicated blockchain node device 23 verifies the digital certificate.

[0058] When verifying the digital certificate, the dedicated blockchain node device 23 needs to use a root certificate generated by the dedicated blockchain node device 22. The dedicated blockchain node device 22 generates the root certificate by the CA service. Specifically, the CA service can sign the CA public key and the description information of the dedicated blockchain node device 22 though the above-mentioned CA private key to generate a digital certificate corresponding to the dedicated blockchain node device 22, i.e. the above-mentioned root certificate. When performing verification for the digital certificate, the dedicated blockchain node device 23 needs to obtain the CA public key from the root certificate and perform signature verification for the digital certificate sent by the dedicated blockchain node device 21 by using the CA public key. If the signature verification is successful, it indicates that the digital certificate is indeed issued by the CA service on the

dedicated blockchain node device 22. Thus, the dedicated blockchain node device 23 can preliminarily determine the dedicated blockchain node device 21 as a blockchain node based on the endorsement of the CA service for the dedicated blockchain node device 21.

[0059] At step 306, the dedicated blockchain node device 23 submits a transaction for adding node in the blockchain network after successful verification, and performs transaction consensus with other blockchain nodes.

[0060] At step 307, after the transaction passes the consensus, the dedicated blockchain node device 23 adds the dedicated blockchain node device 21 as a newly-added node.

[0061] After the dedicated blockchain node device 23 preliminarily determines the dedicated blockchain node device 21 as a blockchain node, other blockchain nodes in the blockchain network also need to accept the dedicated blockchain node device 21. Only in this way can the dedicated blockchain node device 21 be really added as a newly-added node. Therefore, the dedicated blockchain node device 23 can submit a transaction for adding node. The value of the Type field of the transaction can indicate it is a transaction of a node adding type, and the Data field of the transaction can include information of the dedicated blockchain node device 21, for example embodiments, the IP address, the public key of the dedicated node device and the digital certificate and the like of the dedicated blockchain node device 21. After the above-mentioned transaction is submitted, all blockchain nodes in the blockchain network will receive the transaction and further perform consensus for the transaction. If a particular blockchain node accepts the dedicated blockchain node device 21 and agrees to add the dedicated blockchain node device 21 as a newly-added node, the blockchain node can agree to record the above-mentioned transaction in the blockchain. When all blockchain nodes agree to record the transaction in the blockchain, it indicates that the above-mentioned transaction passes consensus. At this time, the dedicated blockchain node device 21 is added as a newly-added node in the blockchain network.

[0062] Each blockchain node in the blockchain network can maintain one node information list to record node information of all blockchain nodes accepted by each blockchain node, such as IP address, public key, and digital certificate of node. In the above-mentioned embodiments, the dedicated blockchain node devices 22-24 respectively maintain node information lists, and respectively add the information of the dedicated blockchain node device 21 to node information lists after the above-mentioned transaction passes consensus, which indicates the dedicated blockchain node device 21 is determined as a newly-added node. Only after the dedicated blockchain node device 21 becomes the newly-added node can the dedicated blockchain node devices 22-24 allow data synchronization with the dedicated blockchain node device 21, where the data synchronization includes blockchain data

synchronization, and status data synchronization. Alternatively, the status data does not have to be synchronized because the dedicated blockchain node device 21 can calculate the status data after obtaining the blockchain data. Further, the dedicated blockchain node device 21 can also synchronize the node information lists maintained by the dedicated blockchain node devices 22-24 so that the node information list maintained by the dedicated blockchain node device 21 is obtained.

[0063] Thus, the dedicated blockchain node devices 21-24 can automatically complete digital certificate issuing and node authentication (based on verification of digital certificate) through the steps of FIG. 3 so that each dedicated blockchain node device determines and records the identified blockchain nodes respectively so as to automatically add the dedicated blockchain node device 21 as a newly-added node in the blockchain network.

[0064] FIG. 4 is a structural schematic diagram of a device according to example embodiments of the present disclosure. As shown in FIG. 4, from hardware level, the device includes a processor 402, an internal bus 404, a network interface 406, a memory 408 and a non-volatile memory 410. Of course, the device can further include hardware needed for other services. The processor 402 reads corresponding computer programs from the non-volatile memory 410 to the memory 408 and then runs the computer programs, so as to logically form an automatic node adding apparatus of a dedicated blockchain node device. Of course, in addition to the software implementation, one or more embodiments of the present disclosure do not preclude other implementations, for example, logic device or a combination of software and hardware or the like. That is, the executing subject of the following processing flow is not limited to each logic unit and can also be hardware or logic device.

[0065] As shown in FIG. 5, in a software implementation, the automatic node adding apparatus can include:

[0066] an address configuring unit 51, configured to enable a dedicated blockchain node device to receive a configuration instruction after accessing a blockchain network, and configure a first network address corresponding to a certificate authority center and a second network address corresponding to a first blockchain node in the blockchain network respectively according to the configuration instruction;

[0067] a certificate requesting unit 52, configured to enable the dedicated blockchain node device to initiate an authentication request to the certificate authority center according to the first network address, and receive a digital certificate returned by the certificate authority center after the certificate authority center determines the authentication request passes verification;

[0068] a certificate sending unit 53, configured to enable the dedicated blockchain node

device to send the digital certificate to the first blockchain node according to the second network address, wherein the digital certificate is used to trigger the first blockchain node to add the dedicated blockchain node device as a newly-added blockchain node in the blockchain network.

[0069] Optionally, the blockchain network is a dedicated network which is accessed by the dedicated blockchain node device via a tunnel.

[0070] Optionally, the certificate authority center is deployed in the blockchain network, or the certificate authority center is deployed in a public network outside the blockchain network.

[0071] Optionally,

[0072] If the certificate authority center is deployed in the blockchain network, the certificate authority center is a blockchain node which has initiated a certificate authority service in the blockchain network.

[0073] If the certificate authority center is deployed in the public network outside the blockchain network, the certificate authority center is deployed on a Blockchain-as-a-Service (BaaS) platform in the public network.

[0074] Optionally, the apparatus further includes:

[0075] an information receiving unit 54, configured to enable the dedicated blockchain node device to receive inquiry information from a second blockchain node in the blockchain network, where the inquiry information is generated and sent by the second blockchain node after automatically discovering the dedicated blockchain node device.

[0076] The certificate sending unit 53 is further configured to enable the dedicated blockchain node device to send the digital certificate to the second blockchain node, where the digital certificate is used to trigger the second blockchain node to add the dedicated blockchain node device as a newly-added blockchain node in the blockchain network.

[0077] Optionally, after the digital certificate is determined as passing verification by any blockchain node in the blockchain network, the digital certificate is used to indicate the any blockchain node to initiate a transaction for adding a node in the blockchain network. The transaction is executed after all blockchain nodes in the blockchain network reach consensus, so that the dedicated blockchain node device is added as a newly-added blockchain node in the blockchain network.

[0078] Optionally, the dedicated blockchain node device is added as a newly-added blockchain node in the blockchain network, including: adding, by all blockchain nodes in the blockchain network, the information of the dedicated blockchain node device into node information lists maintained respectively by all blockchain nodes.

[0079] The systems, apparatuses, modules or units described in the above-mentioned embodiments can be specifically implemented by a computer chip or an entity or can be implemented by a product with a particular function. A typical implementing device can be a computer and the computer can specifically be a personal computer, a laptop computer, a cellular phone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an email transceiver, a game console, a tablet computer, a wearable device, or a combination of any several devices of the above-mentioned devices.

[0080] In a typical configuration, the computer can include one or more central processing units (CPU), an input/output interface, a network interface and a memory.

[0081] The memory can include a non-permanent memory, a random access memory (RAM), and/or a non-volatile memory and the like in a computer readable medium, for example, read only memory (ROM), or flash RAM. The memory is one example of the computer readable medium.

[0082] The computer readable medium includes permanent, non-permanent, mobile and non-mobile media, which can realize information storage by any method or technology. The information can be computer readable instructions, data structures, program modules and other data. The examples of the computer storage medium include but not limited to: a phase change random access memory (PRAM), a Static Random Access Memory (SRAM), a Dynamic Random Access Memory (DRAM), and other types of RAMs, Read-Only Memory (ROM), an Electrically-Erasable Programmable Read-Only Memory (EEPROM), a Flash Memory, or other memory technology, CD-ROM, digital versatile disc (DVD) or other optical storage, cassette type magnetic tape, magnetic disk storage, quantum memory, storage medium based on graphene, or other magnetic storage device or other non-transmission medium for storing information accessible by computing devices. According to the definition of the present disclosure, the computer readable medium does not include transitory computer readable media, for example, modulated data signal and carriers.

[0083] It should be noted that the term “including”, “containing” or any variation thereof is intended to encompass non-exclusive inclusion, so that a process, method, product or device including a series of elements includes not only those elements but also other elements not listed explicitly or those elements inherent to such a process, method, product or device. Without more limitations, an element defined by the statement “including a...” shall not be precluded to include additional same elements present in a process, method, product or device including the elements.

[0084] The specific embodiments are described as above. Other also are within the scope of the appended claims. In some cases, the actions or steps recorded in the claims can be

performed in a sequence different from the examples to achieve the desired result. Further, the processes shown in drawings do not necessarily need a particular sequence or a continuous sequence shown to achieve the desired result. In some examples, a multi-task processing and parallel processing is possible and may also be advantageous.

[0085] The terms used in one or more embodiments of the present disclosure are for the purpose of describing particular examples only, and are not intended to limit the one or more embodiments of the present disclosure. Terms “a”, “the” and “said” used in their singular forms in one or more embodiments of the present disclosure and the appended claims are also intended to include plurality, unless clearly indicated otherwise in the context. It should also be understood that the term “and/or” as used herein refers to and includes any and all possible combinations of one or more of the associated listed items.

[0086] It should be understood that, although the terms “first,” “second,” “third,” and the like may be used in one or more embodiments of the present disclosure to describe various information, such information should not be limited to these terms. These terms are only used to distinguish one category of information from another. For example, without departing from the scope of one or more embodiments of the present disclosure, first information may be referred as second information; and similarly, the second information may also be referred as the first information. Depending on the context, the term “if” as used herein can be interpreted as “when” or “upon” or “in response to determining”.

[0087] The above-mentioned disclosure is merely illustrative of preferred examples of one or more embodiments of the present disclosure but not intended to limit the present disclosure, and any modifications, equivalent substitutions, adaptations thereof made within the spirit and principles of the disclosure shall be encompassed in the scope of protection of the present disclosure.

CLAIMS

1. An automatic node adding method of a dedicated blockchain node device, comprising:

receiving, by the dedicated blockchain node device, a configuration instruction after accessing a blockchain network, and configuring a first network address corresponding to a certificate authority center and a second network address corresponding to a first blockchain node in the blockchain network respectively according to the configuration instruction;

initiating, by the dedicated blockchain node device, an authentication request to the certificate authority center according to the first network address, and receiving a digital certificate returned by the certificate authority center after the certificate authority center determines the authentication request passes verification;

sending, by the dedicated blockchain node device, the digital certificate to the first blockchain node according to the second network address, wherein the digital certificate is used to trigger the first blockchain node to add the dedicated blockchain node device as a newly-added blockchain node in the blockchain network;

receiving, by the dedicated blockchain node device, inquiry information from a second blockchain node in the blockchain network, wherein the inquiry information is generated and proactively sent by the second blockchain node after automatically discovering the dedicated blockchain node device; and

sending, by the dedicated blockchain node device, the digital certificate to the second blockchain node, wherein the digital certificate is used to trigger the second blockchain node to add the dedicated blockchain node device as a newly-added blockchain node in the blockchain network.

2. The method according to claim 1, wherein the blockchain network is a dedicated network which is accessed by the dedicated blockchain node device via a tunnel.

3. The method according to claim 1, wherein,

the certificate authority center is deployed in the blockchain network; or

the certificate authority center is deployed in a public network outside the blockchain network.

4. The method according to claim 3, wherein,

if the certificate authority center is deployed in the blockchain network, the certificate authority center is a blockchain node which has initiated a certificate authority service in the

blockchain network;

if the certificate authority center is deployed in the public network outside the blockchain network, the certificate authority center is deployed on a Blockchain-as-a-Service (BaaS) platform in the public network.

5. The method according to claim 1, wherein,

after the digital certificate is determined as passing verification by any blockchain node in the blockchain network, the digital certificate is used to indicate the any blockchain node to initiate a transaction for adding a node in the blockchain network, and

the transaction is executed after all blockchain nodes in the blockchain network reach consensus, such that adding the dedicated blockchain node device as a newly-added blockchain node in the blockchain network.

6. The method according to claim 1, wherein adding the dedicated blockchain node device as a newly-added blockchain node in the blockchain network comprises:

adding, by all blockchain nodes in the blockchain network, information of the dedicated blockchain node device into node information lists maintained respectively by all blockchain nodes.

7. An automatic node adding apparatus of a dedicated blockchain node device, comprising:

an address configuring unit, configured to enable the dedicated blockchain node device to receive a configuration instruction after accessing a blockchain network, and configure a first network address corresponding to a certificate authority center and a second network address corresponding to a first blockchain node in the blockchain network respectively according to the configuration instruction;

a certificate requesting unit, configured to enable the dedicated blockchain node device to initiate an authentication request to the certificate authority center according to the first network address, and receive a digital certificate returned by the certificate authority center after the certificate authority center determines the authentication request passes verification;

a certificate sending unit, configured to enable the dedicated blockchain node device to send the digital certificate to the first blockchain node according to the second network address, wherein the digital certificate is used to trigger the first blockchain node to add the dedicated blockchain node device as a newly-added blockchain node in the blockchain network; and

an information receiving unit, configured to enable the dedicated blockchain node device to receive inquiry information from a second blockchain node in the blockchain network, wherein the inquiry information is generated and proactively sent by the second blockchain node after automatically discovering the dedicated blockchain node device.

8. A dedicated blockchain node device, comprising:

a processor;

a memory storing instructions executable by the processor;

wherein the processor implements the method according to any one of claims 1-6 by running the executable instructions.

9. A computer readable storage medium for storing computer instructions, wherein the instructions are executed by a processor to implement steps of the method according to any one of claims 1-6.