

CLAIMS

What is claimed is:

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

5 receiving, by one or more processors, a linking request from a node requesting to be linked to a blockchain network, wherein the linking request comprises a to-be-verified digital certificate indicating identity information of the node, and wherein the to-be-verified digital certificate comprises one or more of a validity period of the to-be-verified digital certificate or a version number of the to-be-verified digital certificate;

10 determining a consensus verification result of the to-be-verified digital certificate of the node, comprising:

receiving, by the one or more processors, a plurality of consensus verification messages from a plurality of blockchain nodes of the blockchain network, each consensus verification message indicating whether a respective blockchain node of the plurality of blockchain nodes approves or denies the linking request, wherein each blockchain node of the plurality of blockchain nodes performs a portion of a verification process based on a pre-agreed verification standard, and wherein at least one blockchain node of the plurality of blockchain nodes performs the portion of the verification process by verifying the validity period of the to-be-verified digital certificate;

20 determining, by the one or more processors and based on the plurality of consensus verification messages, a ratio of a total number of blockchain nodes that approve the linking request to a total number of all blockchain nodes in the blockchain network is greater than a threshold number; and

25 in response to determining that the ratio of the total number of blockchain nodes that approve the linking request to the total number of all blockchain nodes in the blockchain network is greater than the threshold number, determining, by the one or more processors, that the linking request is approved by the plurality of blockchain nodes;

determining, based on the consensus verification result, whether to store the to-be-verified digital certificate into the blockchain network, comprising:

30 in response to determining that the consensus verification result comprises the linking request being approved by the plurality of the blockchain nodes,

storing, by the one or more processors, the to-be-verified digital certificate as a digital certificate of the node, wherein the to-be-verified digital certificate is stored into the blockchain network;

receiving, by the one or more processors, a revocation request from a blockchain node of the blockchain network, the revocation request comprising a digital certificate of a target node that is being requested to be revoked;

receiving, by the one or more processors, one or more revocation consensus messages from at least one blockchain node of the blockchain network, each revocation consensus message of the one or more revocation consensus messages indicating whether a respective blockchain node of the at least one blockchain node of the blockchain network approves or denies the revocation request;

determining, by the one or more processors, a revocation consensus result based on the one or more revocation consensus messages;

determining, by the one or more processors and based on the revocation consensus result, that the revocation request is approved by the at least one blockchain node of the blockchain network; and

in response to determining that the revocation request is approved by the at least one blockchain node, revoking, by the one or more processors, the digital certificate of the target node from digital certificates stored in the blockchain network.

2. The method according to claim 1, wherein the node provides the linking request based on a private key of the node.

3. The method according to claim 1, wherein the determining, by the one or more processors and based on the plurality of consensus verification messages, a ratio of a total number of blockchain nodes that approve the linking request to a total number of all blockchain nodes in the blockchain network is greater than a threshold number comprises:

determining, by the one or more processors, that a total number of the plurality of consensus verification messages is greater than a predetermined threshold; and

in response to determining that the total number of the plurality of consensus verification messages exceeds the predetermined threshold, determining, by the one or more processors, the

ratio of the total number of blockchain nodes that approve the linking request to the total number of all blockchain nodes in the blockchain network is greater than the threshold number.

4. An electronic device, wherein the electronic device is applied to a blockchain and
5 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 3.

10

5. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform the method according to any one of claims 1 to 3.

6. A computer-implemented system, comprising:

15

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform the method according to any one of claims 1 to 3.

20