

CLAIMS

What is claimed is:

1. A blockchain-based node management method, wherein a node identity table is stored in a distributed database of a blockchain, and is used to record a certificate of a new blockchain node and a unique identifier that is of the new blockchain node and that corresponds to the certificate, and the method comprises the following:

receiving (102), by an existing node of the blockchain having a node identity table management permission in the blockchain and from the new blockchain node, via an out-of-chain communication, a target transaction, wherein the target transaction comprises the certificate of the new blockchain node and the unique identifier of the new blockchain node;

propagating, by the existing node of the blockchain having the node identity table management permission in the blockchain, the target transaction in the blockchain; and

verifying (104) the target transaction, so that after the target transaction passes consensus verification of the blockchain, the node identity table comprising the unique identifier and the certificate of the new blockchain node is correspondingly recorded to the distributed database of the blockchain.

2. The method according to claim 1, wherein the verifying the target transaction comprises the following:

verifying the certificate of the new blockchain node, and verifying whether a node identity certification authority corresponding to the certificate of the new blockchain node is a node identity certification authority approved by the blockchain.

3. The method according to claim 1, wherein the target transaction further comprises digital signatures created by endorsement nodes of the blockchain based on at least the certificate of the new blockchain node; and

the verifying the target transaction comprises the following:

verifying whether valid digital signatures created by the endorsement nodes of the blockchain based on at least the certificate of the new blockchain node meet a predetermined quantity.

4. The method according to any one of claims 1 to 3, further comprising the following:
- invoking a smart contract corresponding to management of the node identity table, executing update logic of the node identity table stated in the smart contract, verifying the target transaction, and after the verification is passed, correspondingly recording the unique identifier and the certificate of the new blockchain node to the node identity table.
5. The method according to claim 1, further comprising the following:
- receiving (106) a network address of the new blockchain node, the unique identifier of the new blockchain node, and a digital signature created by the new blockchain node;
 - obtaining (108) the node identity table from the distributed database of the blockchain, and obtaining the certificate of the new blockchain node based on the unique identifier;
 - verifying (110) the digital signature based on the certificate of the new blockchain node;
 - and
 - storing (112) the network address in a local database of the existing node of the blockchain after the verification is passed.
6. The method according to claim 5, further comprising the following:
- sending network addresses of other existing nodes of the blockchain stored in the local database of the existing node of the blockchain to the new blockchain node.
7. The method according to claim 5 or 6, further comprising the following:
- sending data in the distributed database of the blockchain backed up by the existing node of the blockchain to the new blockchain node.
8. A computer device, comprising a memory and a processor, wherein the memory stores a computer program that can be executed by the processor, and the processor executes the computer program to perform the method according to any one of claims 1 to 7.
9. A computer readable storage medium, storing a computer program, wherein when the computer program is executed by a processor, the method according to any one of claims 1 to 7 is performed.