

CLAIMS

1. A method for managing digital certificates, the method comprising:
receiving, at a blockchain, a first transaction request sent by a certificate authority,
wherein the first transaction request comprises a request to write a digital certificate issued by
5 the certificate authority to a node in the blockchain into the blockchain;
determining, by the blockchain, a consensus result of consensus verification performed
by the blockchain on the digital certificate, wherein determining the consensus result comprises:
determining verification results of nodes in the blockchain that participate in the
consensus verification on the digital certificate, wherein i) more than half of the nodes in the
10 blockchain participate in the consensus verification on the digital certificate and ii) a number of
nodes in the blockchain that participate in consensus verification on the digital certificate
comprises the number of nodes that complete consensus verification on the digital certificate
within a set duration of consensus verification,
determining a number of first nodes and/or a number of second nodes in the nodes
15 that participate in consensus verification, wherein a first node is a node whose verification result
indicates that consensus verification was successful, and a second node is a node whose
verification result indicates that the consensus verification was not successful, and
determining the consensus result based on the number of first nodes and/or the
number of second nodes; and
20 responding to or rejecting, by the blockchain, the first transaction request based on the
consensus result.
2. The method according to claim 1, wherein determining the verification results of nodes in
the blockchain that participate in the consensus verification on the digital certificate comprises:
25 determining, for each node, an announcement published by the node after the node
performs the consensus verification on the digital certificate, wherein the announcement is used
for broadcasting the first transaction request and the verification result of the node to another
node; and
determining the verification results of the nodes that participate in the consensus
30 verification based on an announcement of each node.

3. The method according to claim 1, wherein determining the consensus result based on the number of first nodes comprises:

determining that the consensus verification on the digital certificate succeeds when the number of first nodes reaches a first predetermined threshold or when a proportion of first nodes in the nodes that participate in the consensus verification reaches a second predetermined threshold.

4. The method according to claim 1, wherein responding to or rejecting the first transaction request based on the consensus result comprises:

responding to the first transaction request to write the digital certificate into the blockchain if the consensus result indicates that the consensus verification was successful; or rejecting the first transaction request if the consensus result indicates that the consensus verification was not successful.

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

receiving a second transaction request sent by the certificate authority, wherein the second transaction request comprises a request to write a certificate revocation list into the blockchain, and the certificate revocation list is used for recording a revoked digital certificate;

determining a consensus result of consensus verification performed by the blockchain on the certificate revocation list; and

responding to or rejecting the second transaction request based on the consensus result.

6. The method according to claim 5, further comprising:

verifying a third transaction request in the blockchain based on the certificate revocation list, wherein the third transaction request is used for requesting to complete a transaction between a first node group and a second node group; and

responding to or rejecting the third transaction request based on a verification result.

7. The method according to claim 6, wherein verifying the third transaction request in the blockchain based on the certificate revocation list comprises:

comparing a digital certificate of a node in the first node group and the second node group with the revoked digital certificate recorded in the certificate revocation list; and
determining the verification result based on a comparison result with reference to a predetermined transaction rule of the transaction.

5

8. The method according to claim 5, further comprising:
receiving a third transaction request sent by the certificate authority, wherein the third transaction request is used for requesting to write update information of the certificate revocation list into the blockchain;

10 determining a consensus result of consensus verification performed by the blockchain on the update information; and

responding to or rejecting the third transaction request based on the consensus result.

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

15 receiving a fourth transaction request sent by the certificate authority, wherein the fourth transaction request comprises a request to write a record of a digital certificate revoked by the certificate authority into the blockchain;

determining a consensus result of consensus verification performed by the blockchain on the record of the revoked digital certificate; and

20 responding to or rejecting the fourth transaction request based on the consensus result.

10. The method according to claim 9, further comprising:

25 constructing a certificate revocation list based on the record of the revoked digital certificate that is written into the blockchain, wherein the certificate revocation list is used for recording the revoked digital certificate.

11. A method for managing digital certificates, the method comprising:

30 receiving, by a certificate authority, an application request sent by a node in a blockchain, wherein the application request is used for requesting a certificate authority to issue a digital certificate to the node;

issuing, by the certificate authority, the digital certificate to the node in response to the application request; and

sending, from the certificate authority, a first transaction request to the blockchain, wherein the first transaction request comprises a request to write the digital certificate into the blockchain, wherein the blockchain performs consensus verification on the digital certificate by:

determining verification results of nodes in the blockchain that participate in the consensus verification on the digital certificate, wherein i) more than half of the nodes in the blockchain participate in the consensus verification on the digital certificate and ii) a number of nodes in the blockchain that participate in the consensus verification on the digital certificate comprises the number of nodes that complete consensus verification on the digital certificate within a set duration of consensus verification,

determining a number of first nodes and/or a number of second nodes in the nodes that participate in the consensus verification, wherein a first node is a node whose verification result indicates that consensus verification was successful, and a second node is a node whose verification result indicates that the consensus verification was not successful,

determining a consensus result based on the number of first nodes and/or the number of second nodes, and

responding to or rejecting the first transaction request based on the consensus result.

12. The method according to any one of claims 1 to 11, wherein the digital certificate comprises at least one of a version, a serial number, a signature algorithm type, issuer information, a validity period, an issuer, an issued public key, and a certificate authority digital signature.

13. The method according to any one of claims 1 to 12, wherein the digital certificate is invalid before being chained in the node of the blockchain.

14. 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 13.