

CLAIMS

What is claimed is:

1. A digital certificate management method, performed by a computer device, the method comprising:

receiving a digital certificate generation request submitted by a certificate application node, the digital certificate generation request carrying identification information of the certificate application node;

transmitting the identification information to consensus authentication centers for certification to obtain certification results obtained by the consensus authentication centers by performing the certification according to the identification information;

determining an identification result corresponding to the certificate application node according to the certification results of the consensus authentication centers;

generating, in a case that the identification result is that the certification succeeds, a target digital certificate corresponding to the certificate application node according to the digital certificate generation request; and

writing the target digital certificate as a transaction resource into a blockchain associated with the consensus authentication centers;

wherein the writing the target digital certificate as a transaction resource into a blockchain associated with the consensus authentication centers comprises:

generating a first certificate transaction record, a transaction resource of the first certificate transaction record being the target digital certificate, a transfer-from account in the first certificate transaction record being a preset initial account, a recipient account in the first certificate transaction record being a certificate issuing account corresponding to a receiving node of the digital certificate generation request; and writing the first certificate transaction record into the blockchain associated with the consensus authentication center.

2. The method according to claim 1, wherein after the writing the target digital certificate as a transaction resource into a blockchain associated with the consensus authentication centers, the method further comprises:

receiving an operation request used for operating the target digital certificate;

determining a recipient account type of receiving the target digital certificate according to an operation type of the operation request; and

generating a second certificate transaction record, and writing the second certificate transaction record into the blockchain, a transaction resource of the second certificate transaction record being the target digital certificate, a recipient account in the second certificate transaction record being a second account corresponding to the recipient account type.

3. The method according to claim 2, wherein the determining a recipient account type of receiving the target digital certificate according to an operation type of the operation request comprises:

determining that the recipient account type is a certificate issuing account type in a case that the operation type of the operation request is an update operation type.

4. The method according to claim 2, wherein the determining a recipient account type of receiving the target digital certificate according to an operation type of the operation request comprises:

determining that the recipient account type is a certificate recovery account type in a case that the operation type of the operation request is a revocation operation type.

5. The method according to any one of claims 1 to 4, wherein after the writing the target digital certificate as a transaction resource into a blockchain associated with the consensus authentication centers, the method further comprises:

receiving a verification request used for verifying the target digital certificate;

obtaining a latest transaction record corresponding to the target digital certificate from the blockchain; and

determining a verification result corresponding to the target digital certificate according to a recipient account type in the latest transaction record.

6. The method according to claim 5, wherein the determining a verification result corresponding to the target digital certificate according to a recipient account type in the latest transaction record comprises:

determining that the target digital certificate is revoked and the verification result corresponding to the target digital certificate indicates that the verification fails in a case that the recipient account type in the latest transaction record is a certificate recovery account type.

7. The method according to claim 5, wherein the determining a verification result

corresponding to the target digital certificate according to a recipient account type in the latest transaction record comprises:

determining that the verification result corresponding to the target digital certificate is that the verification succeeds in a case that the recipient account type in the latest transaction record is a certificate issuing account type.

8. The method according to claim 5, wherein the verification request carries a first transaction identifier corresponding to the first certificate transaction record, and the first transaction identifier is transmitted by a receiving node of the digital certificate generation request to the certificate application node and is then transmitted by the certificate application node to a verification request transmission node.

9. The method according to claim 8, wherein the obtaining a latest transaction record corresponding to the target digital certificate from the blockchain comprises:

obtaining a transaction chain corresponding to the target digital certificate according to the first transaction identifier, and using a transaction record at the end of the transaction chain as the latest transaction record, the transaction chain being sequentially arranged according to transaction time.

10. The method according to claim 5, wherein before the obtaining a latest transaction record corresponding to the target digital certificate from the blockchain, the method further comprises:

obtaining a root certificate corresponding to the target digital certificate from the blockchain according to the verification request, the root certificate being used for verifying identity information of the receiving node of the digital certificate generation request;

verifying the target digital certificate according to the root certificate to obtain a root verification result; and

performing the operations of obtaining a latest transaction record corresponding to the target digital certificate from the blockchain in a case that the root verification result is that the verification succeeds.

11. A digital certificate management apparatus, comprising:

a generation request receiving module, configured to receive a digital certificate generation request submitted by a certificate application node, the digital certificate generation request carrying identification information of the certificate application node;

a consensus certificate module, configured to transmit the identification information to consensus authentication centers for certification to obtain certification results obtained by the

consensus authentication centers by performing the certification according to the identification information;

an identification result obtaining module, configured to determine an identification result corresponding to the certificate application node according to the certification results of the consensus authentication centers;

a certificate generation module, configured to generate a target digital certificate corresponding to the certificate application node according to the digital certificate generation request in a case that the identification result is that the certification succeeds; and

a writing module, configured to write the target digital certificate as a transaction resource into a blockchain associated with the consensus authentication centers in a case that the identification result is that the certification succeeds;

wherein the writing module comprises: a first record generation unit, configured to generate a first certificate transaction record, a transaction resource of the first certificate transaction record being the target digital certificate, a transfer-from account in the first certificate transaction record being a preset initial account, a recipient account in the first certificate transaction record being a certificate issuing account corresponding to a receiving node of the digital certificate generation request; and a first writing unit, configured to write the first certificate transaction record into the blockchain associated with the consensus authentication center.

12. The apparatus according to claim 11, wherein the apparatus further comprises:

an operation request receiving module, configured to receive an operation request used for operating the target digital certificate;

an account type determination module, configured to determine a recipient account type of receiving the target digital certificate according to an operation type of the operation request; and

a second transaction record generation module, configured to: generate a second certificate transaction record, and write the second certificate transaction record into the blockchain, a transaction resource of the second certificate transaction record being the target digital certificate, a recipient account in the second certificate transaction record being a second account corresponding to the recipient account type.

13. A computer device, comprising a memory and a processor, the memory storing a computer program, and the computer program, when executed by the processor, causing the processor to

perform the operations of the digital certificate management method according to any one of claims 1 to10.

14. A computer-readable storage medium, storing a computer program, the computer program, when executed by a processor, causing the processor to perform the operations of the digital certificate management method according to any one of claims 1 to10.