

[0006] One aspect of the present disclosure provides a digital certificate verification method. The method includes receiving a verification request for verifying a target digital certificate; obtaining a target transaction record corresponding to the target digital certificate from a blockchain, the target digital certificate being stored in the blockchain as a transaction resource; obtaining a target account type corresponding to the target transaction record, different account types corresponding to different certificate operation states; and determining a verification result corresponding to the target digital certificate according to the target account type.

[0007] Another aspect of the present disclosure provides a digital certificate verification apparatus in an authentication center. The apparatus includes a verification request receiving module, configured to receive a verification request for verifying a target digital certificate; a target transaction record obtaining module, configured to obtain a target transaction record corresponding to the target digital certificate from a blockchain, the target digital certificate being stored in the blockchain as a transaction resource; a target account type obtaining module, configured to obtain a target account type corresponding to the target transaction record, different account types corresponding to different certificate operation states; and a verification result determination module, configured to determine a verification result corresponding to the target digital certificate according to the target account type.

[0008] In one embodiment, the apparatus further includes: an operation request receiving module, configured to receive an operation request for operating the target digital certificate; a recipient account type determination module, configured to determine a target recipient account type corresponding to the target digital certificate according to an operation type of the operation request; and a certificate transaction record generation module, configured to: generate a certificate transaction record corresponding to the operation request, and write the certificate transaction record into the blockchain, a transaction resource in the certificate transaction record being the target digital certificate, a recipient account in the certificate transaction record being an account corresponding to the target recipient account type.

[0009] In one embodiment, the recipient account type determination module is configured to determine that the target recipient account type is a certificate issuing account type if the operation type corresponding to the operation request is an update operation type or an insertion operation type.

[0010] In one embodiment, the recipient account type determination module is configured to determine that the target recipient account type is a certificate recovery account type if the operation type corresponding to the operation request is a revocation operation type.

[0100] In one embodiment, it may be alternatively determined whether the target digital certificate exists in the blockchain. If the target digital certificate exists in the blockchain, the verification of the target digital certificate succeeds. Because a digit of a blockchain is not prone to tampering, if a consistent digital certificate exists in the blockchain, it indicates that the digital certificate is trustworthy.

[0101] FIG. 9 is a diagram of an application environment of a digital certificate verification method according to an embodiment. The application environment includes an authentication center 1, an authentication center 2, an authentication center 3, and an authentication center 4 that belong to a same blockchain and a certificate application node. The certificate verification method provided in this embodiment of this application is described below with reference to FIG. 9.

[0102] 1. When it is necessary to apply for a digital certificate, the certificate application node transmits a digital certificate generation request to the authentication center 1, the digital certificate generation request carrying identity certification information.

[0103] 2. The authentication center 1 receives the digital certificate generation request, and transmits the identity certification information to the authentication center 2, the authentication center 3, and the authentication center 4, to perform consensus authentication.

[0104] 3. When an identity certification result obtained according to a result of the consensus authentication is that the certification succeeds, the authentication center 1 generates a target digital certificate and a corresponding first transaction record, stores the first transaction record in the latest block in a blockchain, and returns the target digital certificate and a first transaction identifier to the certificate application node.

[0105] 4. When interacting with the certificate application node, an interaction node transmits a digital certificate obtaining request to the certificate application node.

[0106] 5. The certificate application node returns the target digital certificate and the first transaction identifier to the interaction node.

[0107] 6. The interaction node transmits a verification request to the authentication center 4, the verification request carrying the first transaction identifier and the target digital certificate.

[0108] 7. The authentication center 4 obtains a root certificate from a genesis block, and verifies the target digital certificate according to the root certificate to obtain a root verification result.

[0109] 8. When the root verification succeeds, the authentication center 4 obtains a recipient account type in a latest transaction record in a transaction chain corresponding to the target digital