

DIGITAL CERTIFICATE PROCESSING METHOD AND RELATED APPARATUS

ABSTRACT

Embodiments of the present application disclose a digital certificate processing method and apparatus. The method includes: recording, by a CA of a first participant in a blockchain network, a CA public key of the first participant in the blockchain network; when receiving a certificate authorization request of any user, confirming, by the CA of the first participant based on user identity information carried in the certificate authorization request, whether the user is a user of the CA of the first participant; if yes, obtaining a public key of the user from the certificate authorization request, and obtaining CA public keys of any N second participants from the blockchain network based on a ring signature certificate issuing rule, where N is equal to a public key quantity that is set in the ring signature certificate issuing rule; and performing, by the CA of the first participant, ring signature on the user identity information and the public key of the user based on the public key and a private key of the CA of the first participant and the CA public keys of the N second participants and forming a digital certificate; and sending the digital certificate to the user. Identity privacy of a digital certificate issuer can be enhanced by using the embodiments of the present application.

Fig. 2 accompanies abstract