

METHOD AND APPARATUS FOR IMPLEMENTING SECURE MULTICAST IN BLOCKCHAIN NETWORK

ABSTRACT

One or more embodiments of this specification provide a method and an
5 apparatus for implementing secure multicast in a blockchain network. The method
includes: a first blockchain node generates and sends a security group creation
message, where the security group creation message includes a security group
information structure corresponding to each target blockchain node to be added to a
multicast security group, each security group information structure includes a public
10 key of a corresponding target blockchain node and ciphertext security group
information obtained by encrypting plaintext security group information by using the
public key, the plaintext security group information includes a security group session
key, and the security group session key is used to encrypt a multicast message in the
multicast security group for transmission; and a second blockchain node searches,
15 after receiving the security group creation message, the security group creation
message for a security group information structure that includes a public key of the
second blockchain node, and decrypts, by using a private key of the second
blockchain node, ciphertext security group information in the identified security group
information structure to obtain the security group session key.

20

(FIG. 1)