

Blockchain-Based Secure Transaction Method, Electronic Device, System and Storage Medium

Abstract

The invention relates to a blockchain-based secure transaction method, electronic device, system and storage medium. The method includes the steps of: a supervisor writes a digital certificate and a corresponding first public key into an intelligent contract of a blockchain corresponding to an asset type to be supervised, so that all institutions with asset accounts under the asset type can obtain the first public key of the supervisor through the digital certificate, so as to generate an additive homomorphic key for homomorphic encryption of the balance of an asset account; when checking the balance of a new account of a transactor, the supervisor obtains a public key in a public-private key pair corresponding to the new account, generates an additive homomorphic key based on a supervision private key corresponding to the supervisor and a predetermined key exchange protocol and the public key in the public-private key pair according to the key exchange protocol, and decrypts the encrypted balance of the new account by using the generated additive homomorphic key. The invention can effectively ensure the security of the account and supervise the account in blockchain-based transaction, and can also improve the efficiency of transaction processing.

Figure 2