CLAIMS

1. A blockchain integrated station comprising a smart contract processing chip and a cryptographic acceleration card assembled thereon,

wherein the smart contract processing chip is configured to process a smart contract and complete key negotiation with a provider for the provider to encrypt and transmit a node private key of a blockchain node to the smart contract processing chip based on a negotiated key;

wherein the cryptographic acceleration card comprises:

a collecting module, configured to collect and output hardware feature data of the blockchain integrated station to a key generating module in response to receiving a key generation request, the key generation request based on a request of a hardware root-of-trust key;

the key generating module, configured to generate an identity key of the blockchain integrated station according to the hardware feature data of the blockchain integrated station, wherein the identity key comprises an identity private key and an identity public key, wherein the identity private key is the hardware root-of-trust key and corresponds to the identity public key; and

an encrypting and decrypting module, configured to be connected to the key generating module to encrypt the identity private key into a private key ciphertext for storage;

wherein the cryptographic acceleration card is configured to maintain the hardware root-of-trust key, perform signature operation based on the hardware root-of-trust key and assist the smart contract processing chip to complete the key negotiation with the provider.

2. The blockchain integrated station according to claim 1, wherein the blockchain integrated station further comprises a master control chip and the hardware feature data is feature data of the master control chip.

3. The blockchain integrated station according to claim 1, wherein the hardware feature data is feature data of one or more of the smart contract processing chip or an intelligent network card comprised in the blockchain integrated station.

4. The blockchain integrated station according to claim 1, wherein, during the key negotiation, the smart contract processing chip is configured to send negotiation information signed using the hardware root-of-trust key to the provider for the provider to verify a signature of the negotiation information based on the identity public key and, after successful signature

verification, negotiate the negotiated key with the smart contract processing chip based on the negotiation information,

wherein the signature operation of the negotiation information is performed by the cryptographic acceleration card based on the hardware root-of-trust key.

5. The blockchain integrated station according to claim 1, the cryptographic acceleration card further comprising:

a signing module, configured to call the encrypting and decrypting module to decrypt the private key ciphertext in response to receiving an identity verification request, and sign to-be-signed data provided by the blockchain integrated station according to the identity private key obtained by decryption.

6. The blockchain integrated station according to claim 1, the cryptographic acceleration card further comprising:

a storing module, configured to store the private key ciphertext output by the encrypting and decrypting module, wherein the storing module is preferably a One Time Programmable, OTP, memory.

7. The blockchain integrated station according to claim 1, wherein the encrypting and decrypting module is further configured to output the private key ciphertext to a storage space outside the cryptographic acceleration card for storage.

8. The blockchain integrated station according to claim 1, wherein the smart contract processing chip is configured to deploy the node private key of the blockchain node to satisfy privacy transaction needs in a blockchain scenario and the node private key of the blockchain node corresponds to a node public key to be used by a client device for performing encrypted transmission of blockchain transaction to the blockchain node, which is configured to perform decryption through the node private key.

9. A key management method of a blockchain integrated station, the blockchain integrated station comprising a smart contract processing chip and a cryptographic acceleration card assembled thereon, wherein the smart contract processing chip is configured to process a smart contract and complete key negotiation with a provider for the provider to encrypt and transmit a node private key of a blockchain node to the smart contract processing chip based on a negotiated key, wherein the method is performed by the cryptographic acceleration card and comprises:

in response to receiving a key generation request based on a request of a hardware

root-of-trust key, collecting hardware feature data of the blockchain integrated station;

generating an identity key of the blockchain integrated station, according to the hardware feature data, wherein the identity key comprises an identity private key and an identity public key and the identity private key is the hardware root-of-trust key and corresponds to the identity public key;

encrypting the identity private key into a private key ciphertext; and

storing the private key ciphertext;

wherein the cryptographic acceleration card is configured to maintain the hardware root-of-trust key, perform signature operation based on the hardware root-of-trust key and assist the smart contract processing chip to complete the key negotiation with the provider.

10. The key management method according to claim 9, wherein the blockchain integrated station further comprises a master control chip and the hardware feature data is feature data of the master control chip.

11. The key management method according to claim 9, wherein the hardware feature data is feature data of one or more of the smart contract processing chip or an intelligent network card comprised in the blockchain integrated station.

12. The key management method according to claim 9, wherein, during the key negotiation, the smart contract processing chip is configured to send negotiation information signed using the hardware root-of-trust key to the provider for the provider to verify a signature of the negotiation information based on the identity public key and, after successful signature verification, negotiate the negotiated key with the smart contract processing chip based on the negotiation information,

wherein the signature operation of the negotiation information is performed by the cryptographic acceleration card based on the hardware root-of-trust key.

13. The key management method according to claim 9, further comprising:

decrypting the private key ciphertext in response to receiving an identity verification request, and signing to-be-signed data provided by the blockchain integrated station according to the identity private key obtained by decryption.

14. The key management method according to claim 9, wherein storing the private key ciphertext comprises:

storing the private key ciphertext to a storage space inside the cryptographic acceleration

card.

15. The key management method according to claim 9, wherein storing the private key ciphertext comprises:

storing the private key ciphertext to a storage space outside the cryptographic acceleration card.

16. The key management method according to claim 9, wherein the smart contract processing chip is configured to deploy the node private key of the blockchain node to satisfy privacy transaction needs in a blockchain scenario and the node private key of the blockchain node corresponds to a node public key to be used by a client device for performing encrypted transmission of blockchain transaction to the blockchain node, which is configured to perform decryption through the node private key.

17. A computer readable storage medium on a cryptographic acceleration card assembled on a blockchain integrated station, the blockchain integrated station comprising the cryptographic acceleration card and a smart contract processing chip and the medium having computer instructions stored thereon, which, when executed by a processor (402) of the cryptographic acceleration card, cause the cryptographic acceleration card to implement steps in a method according to any of claims 9-16.