CLAIMS

What is claimed is:

1. A payment method for a near field communication (NFC) portable device, comprising:

obtaining, by the NFC portable device, NFC writing information, wherein the NFC writing information comprises a key pair identifier and a public key corresponding to the key pair identifier;

when entering the NFC communication range of a consumption machine, receiving expense information sent by the consumption machine;

encrypting the expense information by using the public key to obtain encrypted information; and

sending the encrypted information and the key pair identifier to the consumption machine, wherein after decrypting the encrypted information, a server deducts, based on the expense information, money from a user account that is pre-associated with the key pair identifier.

2. The method according to claim 1, wherein the server generates in advance the key pair identifier and a key pair corresponding to the key pair identifier, and sends the key pair identifier and the public key in the key pair, and wherein an NFC writing end writes the sent information into the NFC portable device.

3. The method according to claim 1, wherein the NFC writing information further comprises account identification information of the user account associated with the key pair identifier, and wherein sending the encrypted information and the key pair identifier to the consumption machine further comprises:

sending the account identification information to the consumption machine for the server to find a private key for the decryption in the key pair.

4. The method according to claim 1, wherein the encrypting the expense information by using the public key to obtain encrypted information comprises:

obtaining a current time; and

encrypting the expense information and the current time by using the public key to obtain the encrypted information, wherein the current time is used by the server to

perform timeliness verification before the deduction.

5. The method according to any one of claims 1 to 4, wherein the NFC portable device is an NFC-enabled wearable device or a card.

6. A payment method based on a near field communication NFC portable device, comprising:

when the NFC portable device enters the NFC communication range of a consumption machine, sending, by the consumption machine, expense information to the NFC portable device;

receiving, from the NFC portable device, a key pair identifier and encrypted information obtained by encrypting the expense information by using a public key corresponding to the key pair identifier, wherein the key pair identifier and the public key are written into the NFC portable device in advance; and

sending the encrypted information and the key pair identifier to a server, wherein after decrypting the encrypted information, the server deducts, based on the expense information, money from a user account that is pre-associated with the key pair identifier.

7. The method according to claim 6, wherein the receiving a key pair identifier and encrypted information obtained by encrypting the expense information by using a public key corresponding to the key pair identifier further comprises:

receiving account identification information of the user account sent by the NFC portable device, wherein the account identification information is written into the NFC portable device in advance; and

the sending the encrypted information and the key pair identifier to a server further comprises:

sending the account identification information to the server for finding a private key for the decryption in the key pair.

8. The method according to claim 6, wherein the sending the encrypted information and the key pair identifier to a server further comprises:

sending corresponding business scenario information to the server to generate a corresponding business receipt.

9. A payment apparatus based on a near field communication NFC portable device, wherein the apparatus is located in the NFC portable device and comprises:

an acquisition module, configured to obtain NFC writing information, wherein the NFC writing information comprises a key pair identifier and a public key corresponding to the key pair identifier;

a receiving module, configured to: when entering the NFC communication range of a consumption machine, receive expense information sent by the consumption machine;

an encryption module, configured to encrypt the expense information by using the public key to obtain encrypted information; and

a sending module, configured to send the encrypted information and the key pair identifier to the consumption machine, wherein after decrypting the encrypted information, a server deducts, based on the expense information, money from a user account that is pre-associated with the key pair identifier.

10. The apparatus according to claim 9, wherein the server generates in advance the key pair identifier and the key pair corresponding to the key pair identifier, and sends the key pair identifier and the public key in the key pair, and wherein an NFC writing end writes the sent information into the NFC portable device.

11. The apparatus according to claim 9, wherein the NFC writing information further comprises account identification information of the user account associated with the key pair identifier; and

that the sending module sends the encrypted information and the key pair identifier to the consumption machine further comprises:

the sending module sends the account identification information to the consumption machine for the server to find a private key for the decryption in the key pair.

12. The apparatus according to claim 9, wherein that the encryption module encrypts the expense information by using the public key to obtain the encrypted information comprises:

the encryption module obtains a current time; and

encrypts the expense information and the current time by using the public key to obtain the encrypted information,

wherein the current time is used by the server to perform timeliness verification before the deduction.

13. The apparatus according to any one of claims 9 to 12, wherein the NFC portable device is an NFC-enabled wearable device or a card.

14. A payment apparatus based on a near field communication NFC portable device, wherein the apparatus is located in a consumption machine and comprises:

a first sending module, configured to: when the NFC portable device enters the NFC communication range of the consumption machine, send expense information to the NFC portable device;

a receiving module, configured to receive, from the NFC portable device, a key pair identifier and encrypted information obtained by encrypting the expense information by using a public key corresponding to the key pair identifier, wherein the key pair identifier and the public key are written into the NFC portable device in advance; and

a second sending module, configured to send the encrypted information and the key pair identifier to a server, wherein after decrypting the encrypted information, the server deducts, based on the expense information, money from a user account that is pre-associated with the key pair identifier.

15. The apparatus according to claim 14, wherein that the receiving module receives, from the NFC portable device, the key pair identifier and the encrypted information obtained by encrypting the expense information by using the public key corresponding to the key pair identifier further comprises:

the receiving module receives account identification information of the user account sent by the NFC portable device, wherein the account identification information is written into the NFC portable device in advance;

wherein that the second sending module sends the encrypted information and the key pair identifier to the server further comprises:

the second sending module sends the account identification information to the server for finding a private key for the decryption in the key pair.

16. The apparatus according to claim 14, wherein that the second sending

module sends the encrypted information and the key pair identifier to the server further comprises:

the second sending module sends corresponding business scenario information to the server to generate a corresponding business receipt.

17. A payment device based on a near field communication NFC portable device, wherein the device is the NFC portable device and comprises:

at least one processor; and

at least one memory communicatively connected to the at least one processor; wherein

the memory stores an instruction that can be executed by the at least one processor, and the instruction is executed by the at least one processor to enable the at least one processor to:

obtain NFC writing information, wherein the NFC writing information comprises a key pair identifier and a public key corresponding to the key pair identifier;

when entering the NFC communication range of a consumption machine, receive expense information sent by the consumption machine;

encrypt the expense information by using the public key to obtain encrypted information; and

send the encrypted information and the key pair identifier to the consumption machine, wherein after decrypting the encrypted information, a server deducts, based on the expense information, money from a user account that is pre-associated with the key pair identifier.

18. A payment device based on a near field communication NFC portable device, wherein the device is a consumption machine and comprises:

at least one processor; and

at least one memory communicatively connected to the at least one processor; wherein

the memory stores an instruction that can be executed by the at least one processor, and the instruction is executed by the at least one processor to enable the at least one processor to:

when the NFC portable device enters an NFC communication range of the consumption machine, send expense information to the NFC portable device;

receive, from the NFC portable device, a key pair identifier and encrypted information obtained by encrypting the expense information by using a public key corresponding to the key pair identifier, wherein the key pair identifier and the public key are written into the NFC portable device in advance; and

send the encrypted information and the key pair identifier to a server, wherein after decrypting the encrypted information, the server deducts, based on the expense information, money from a user account that is pre-associated with the key pair identifier.