CLAIMS

What is claimed is:

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

obtaining (S202), by the NFC portable device from a server, NFC writing information, wherein the NFC writing information comprises a key pair identifier, a public key corresponding to the key pair identifier, and account identification information of a user account associated with the key pair identifier;

when entering an NFC communication range of a consumption machine, receiving (S204) expense information sent by the consumption machine;

encrypting (S206) the expense information by using the public key to obtain encrypted information, comprising:

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 a deduction; and

sending (S208) the encrypted information, the key pair identifier, and the account identification information to the consumption machine for the server to find a private key ~~for decryption~~ in a key pair for decrypting the encrypted information, based on the account identification information, wherein after decrypting the encrypted information, the server deducts, based on the expense information, money from the 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 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.~~

~~4~~3. The method according to any one of claims 1 to ~~3~~2, wherein the NFC portable device is an NFC-enabled wearable device or a card.

~~5~~4. A payment method based on a near field communication, NFC, portable device, comprising:

when the NFC portable device enters an NFC communication range of a consumption machine, sending (S402), by the consumption machine, expense information to the NFC portable device;

receiving (S404), by the consumption machine from the NFC portable device, a key pair identifier, encrypted information obtained by encrypting the expense information and a current time obtained by the NFC portable device by using a public key corresponding to the key pair identifier, and account identification information of a user account, wherein the key pair identifier, the public key, and the account identification information are written into the NFC portable device in advance; and

sending (S406), by the consumption machine, the encrypted information, the key pair identifier, and the account identification information to a server for finding a private key ~~for decryption~~ in a key pair for decrypting the encrypted information, based on the account identification information, wherein after decrypting the encrypted information, the server deducts, based on the expense information, money from the user account that is pre-associated with the key pair identifier, and wherein the server uses the current time to perform timeliness verification before the deduction.

~~6~~5. The method according to claim ~~5~~4, 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.

~~7~~6. A payment method based on a near field communication, NFC, portable device, comprising:

generating, by a server, a key pair identifier and a key pair;

associating, by the server, the key pair identifier and the key pair with a user account;

sending, by the server, the key pair identifier and a public key in the key pair, wherein an NFC writing end writes the sent information into the NFC portable device;

receiving (S502), by the server from a consumption machine, the sent key pair identifier ~~sent~~, encrypted information that comprises expense information, and account identification information of the user account, wherein the encrypted information is generated by the NFC portable device by using the public key corresponding to the key pair identifier, and is sent to the consumption machine by using an NFC communication method;

determining (S504), based on the account identification information the key pair identifier, a private key corresponding to the key pair identifier, and decrypting the encrypted information by using the private key to obtain the expense information; ~~and~~

determining effectiveness of the current time based on a time of the server;

and in response to positively determining the effectiveness of the current time based on the time of the server, deducting (S506), based on the expense information, money from the user account that is pre-associated with the key pair identifier.

~~8. The method according to claim 7, wherein the encrypted information further comprises a current time obtained by the NFC portable device; and~~

~~before the deducting, based on the expense information, money from a user account that is pre-associated with the key pair identifier, the method further comprises:~~

~~determining effectiveness of the current time based on a time of the server.~~

~~9~~7. A device comprising modules being configured to perform a method according to any one of the preceding claims.