

CLAIMS

What is claimed is:

1. An electronic cash-based offline transaction method, comprising:

receiving, by a back-end server from a smart card, an anti-replay factor generated by the smart card, wherein the smart card is a transaction device at a payment end, and the anti-replay factor generated by the smart card is a random number;

determining, by the back-end server in accordance with a predetermined algorithm, whether an abnormal transaction occurs on the smart card, generating, by the back-end server when no abnormal transaction occurs, a security information signature by signing security information with a private key of the back-end server, and transmitting, by the back-end server, the security information and the security information signature to the smart card, wherein the security information at least comprises an anti-replay factor and active field information, and the active field information at least comprises a term of validity of the smart card or an upper limit of a transaction amount;

receiving, by the smart card, the security information and the security information signature from the back-end server, performing a signature verification, by the smart card, on the security information signature by using a public key of the back-end server, determining, by the smart card after the signature verification succeeds, whether the anti-replay factor in the security information is consistent with the anti-replay factor generated by the smart card, and storing, by the smart card, the active field information, when the anti-replay factor in the security information is consistent with the anti-replay factor generated by the smart card;

establishing, by a transaction terminal, a connection with the smart card, and transmitting, by the transaction terminal, application selection information of an electronic cash transaction to the smart card, when no connection is established between the transaction terminal and the back-end server;

receiving, by the smart card, the application selection information of the electronic cash transaction, determining, by the smart card, that an application for the electronic cash transaction is activated, and transmitting, by the smart card, the active field information to the transaction terminal, when no connection is established between the smart card and the back-end server;

generating, by the transaction terminal, transaction information, and determining, by the transaction terminal, whether the active field information is in a valid state, wherein the

transaction information at least comprises the transaction amount;

terminating a transaction process, when the active field information is invalid;

transmitting the transaction information to the smart card, when the active field information is valid;

deducting, by the smart card after receiving the transaction information, the transaction amount in the transaction information from a balance in the smart card, obtaining, by the smart card, a transaction receipt by calculating the transaction information, and transmitting, by the smart card, the transaction receipt to the transaction terminal; and

establishing, by the smart card, the connection with the back-end server, generating, by the smart card, the anti-replay factor, and transmitting, by the smart card, the anti-replay factor to the back-end server.

2. The method according to claim 1, wherein when the active field information comprises the upper limit of the transaction amount, said determining, by the transaction terminal, whether the active field information is in the valid state comprises:

determining, by the transaction terminal, whether the transaction amount in the transaction information is smaller than or equal to the upper limit of the transaction amount, wherein when the transaction amount is small than or equal to the upper limit of the transaction amount, the active field information is valid, and when the transaction amount is greater than the upper limit of the transaction amount, the active field information is invalid.

3. The method according to claim 1, wherein when the active field information comprises the term of validity of the smart card, said determining, by the transaction terminal, whether the active field information is in the valid state comprises:

obtaining, by the transaction terminal, transaction time, and determining, by the transaction terminal, whether the transaction time is within the term of validity of the smart card, wherein when the transaction time is within the term of validity of the smart card, the active field information is valid, and when the transaction time is not within the term of validity of the smart card, the active field information is invalid.

4. The method according to any one of claims 1 to 3, further comprising:

generating, by the smart card after establishing the connection with the back-end server, transaction settlement information based on electronic cash stored in the smart card and all transaction receipts generated when no connection is established between the smart card and the back-end server, and transmitting, by the smart card, the transaction settlement information to the back-end server, wherein each transaction settlement information at least comprises at least one transaction receipt; and

receiving, by the back-end server, the transaction settlement information from the smart card, and performing electronic cash settlement, by the back-end server, based on the transaction settlement information.

5. The method according to claim 4, further comprising, subsequent to said receiving, by the back-end server, the transaction settlement information from the smart card, and performing the electronic cash settlement, by the back-end server, based on the transaction settlement information:

issuing, by the back-end server, new electronic cash to the smart card; and

receiving and storing, by the smart card, the new electronic cash, and adding, by the smart card, a denomination of the new electronic cash to the balance in the smart card.

6. The method according to claim 5, wherein said determining, by the back-end server in accordance with the predetermined algorithm, whether the abnormal transaction occurs on the smart card comprises:

receiving, by the back-end server, the transaction settlement information transmitted by the smart card, determining, by the back-end server, whether a total transaction amount of all transaction information generated when no connection is established between the smart card and the back-end server is greater than a denomination of the electronic cash stored in the smart card, and determining, by the back-end server, that the abnormal transaction occurs on the smart card, when the total transaction amount of all transaction information generated when no connection is established between the smart card and the back-end server is greater than the denomination of the electronic cash stored in the smart card.

7. An electronic cash-based offline transaction system, comprising:

a back-end server;

a smart card; and

a transaction terminal,

wherein the back-end server is configured to receive from a smart card an anti-replay factor generated by the smart card, determine whether an abnormal transaction occurs on the smart card in accordance with a predetermined algorithm, generate a security information signature by signing security information with a private key of the back-end server, when no abnormal transaction occurs, and transmit the security information and the security information signature to the smart card, wherein the smart card is a transaction device at a payment end, and the anti-replay factor generated by the smart card is a random number, the security information at least comprises an anti-replay factor and active field information, and the active field information at least comprises a term of validity of the smart card or an upper

limit of a transaction amount;

the smart card is configured to receive the security information and the security information signature from the back-end server, perform a signature verification on the security information signature by using a public key of the back-end server, determine, after the signature verification succeeds, whether the anti-replay factor in the security information is consistent with the anti-replay factor generated by the smart card, and store the active field information, when the anti-replay factor in the security information is consistent with the anti-replay factor generated by the smart card;

the transaction terminal is configured to establish a connection with the smart card, and transmit application selection information of an electronic cash transaction to the smart card, when no connection is established between the transaction terminal and the back-end server;

the smart card is further configured to receive the application selection information of the electronic cash transaction, determine that an application for the electronic cash transaction is activated, and transmit the active field information to the transaction terminal, when no connection is established between the smart card and the back-end server;

the transaction terminal is further configured to generate transaction information, determine whether the active field information is in a valid state, terminate a transaction process when the active field information is invalid, and transmit the transaction information to the smart card when the active field information is valid, wherein the transaction information at least comprises the transaction amount; and

the smart card is further configured to deduct the transaction amount in the transaction information from a balance in the smart card after receiving the transaction information, obtain a transaction receipt by calculating the transaction information, transmit the transaction receipt to the transaction terminal, establish a connection with the back-end server, generate the anti-replay factor, and transmit the anti-replay factor to the back-end server.

8. The system according to claim 7, wherein when the active field information comprises the upper limit of the transaction amount, the transaction terminal is further configured to determine whether the transaction amount in the transaction information is smaller than or equal to the upper limit of the transaction amount, wherein when the transaction amount is smaller than or equal to the upper limit of the transaction amount, the active field information is valid, and when the transaction amount is greater than the upper limit of the transaction amount, the active field information is invalid.

9. The system according to claim 7, wherein when the active field information comprises the term of validity of the smart card, the transaction terminal is further configured

to obtain transaction time and determine whether the transaction time is within the term of validity of the smart card, wherein when the transaction time is within the term of validity of the smart card, the active field information is valid, and when the transaction time is not within the term of validity of the smart card, the active field information is invalid.

10. The system according to any one of claims 7 to 9, wherein the smart card is further configured to generate, after the smart card establishes the connection with the back-end server, transaction settlement information based on electronic cash stored in the smart card and all transaction receipts generated when no connection is established between the smart card and the back-end server, and transmit the transaction settlement information to the back-end server, wherein each transaction settlement information at least comprises at least one transaction receipt; and

the back-end server is further configured to receive the transaction settlement information from the smart card, and perform electronic cash settlement based on the transaction settlement information.

11. The system according to claim 10, wherein the back-end server is further configured to issue new electronic cash to the smart card; and

the smart card is further configured to receive and store the new electronic cash, and add a denomination of the new electronic cash to the balance in the smart card.

12. The system according to claim 11, wherein the back-end server being configured to determine whether the abnormal transaction occurs on the smart card in accordance with the predetermined algorithm comprises:

the back-end server being further configured to receive the transaction settlement information transmitted by the smart card, and determine whether a total transaction amount of all transaction information generated when no connection is established between the smart card and the back-end server is greater than a denomination of the electronic cash stored in the smart card, and determine that the abnormal transaction occurs on the smart card, when the total transaction amount of all transaction information generated when no connection is established between the smart card and the back-end server is greater than the denomination of the electronic cash stored in the smart card.