

CLAIMS

What is claimed is:

1. An offline electronic currency collection method, comprising:

5 controlling, by a second security control module, a second communication module to establish a wireless connection with a first device;

 receiving, by the second security control module, wallet information through the second communication module, wherein the wallet information comprises first device offline account information, a first device available balance and a first device electronic currency, wherein the
10 first device electronic currency at least comprises the following fields: a currency denomination, an owner identification, and an issuer signature;

 performing a verification operation and passing of the verification by the second security control module, wherein the verification operation comprises: verifying whether the first device offline account information is included in an offline transaction blacklist stored in a second file
15 storage module, verifying whether the first device electronic currency is legal, and verifying whether the first device available balance is smaller than or equal to a total denomination of the first device electronic currency; and the passing of the verification comprises: verifying that the first device offline account information is not included in the offline transaction blacklist stored in the second file storage module, verifying that the first device electronic currency is legal, and
20 verifying that the first device available balance is smaller than or equal to the total denomination of the first device electronic currency;

 transmitting, by the second security control module after the passing of the verification, collection information to the first device, wherein the collection information at least comprises self offline account information acquired from the second file storage module;

25 receiving, by the second security control module, first transaction data through the second communication module, wherein the first transaction data is generated after the first device verifies that the self offline account information is not included in an offline transaction blacklist stored in the first device; the first transaction data at least comprises first transaction

information and first signature information obtained by digitally signing the first transaction information; and the first transaction information at least comprises the first device offline account information, the self offline account information, first transaction time and a first transaction amount; and

5 verifying, by the second security control module, the first signature information in accordance with the first transaction information and a public key of the first device; controlling, by the second security control module in response to passing of the verifying, the second file storage module to set a current in-transit balance to a first balance, and controlling the storage module to store a first transaction record comprising the first transaction data, wherein the first
10 balance is a balance obtained by adding the first transaction amount to an original in-transit balance.

2. The method according to claim 1, further comprising:

performing an online connection, by the second security control module, with a back end through the second communication module, transmitting the first transaction record, the first
15 balance and an original self offline balance to the back end, receiving a new self electronic currency issued by the back end after the back end confirms that the first transaction record, the first balance and the original self offline balance are correct, and controlling the second file storage module to store the new self electronic currency; deleting all electronic currencies stored in the second file storage module, and setting the current in-transit balance to zero and a
20 current self offline balance to a denomination of the new self electronic currency, wherein the denomination of the new self electronic currency is equal to a sum of the first balance and the original self offline balance.

3. The method according to claim 1, wherein,

the first device available balance comprises a first device offline balance; and

25 the first device electronic currency comprises a first device offline electronic currency.

4. The method according to claim 1, wherein,

the first device available balance comprises the first device offline balance and the first device in-transit balance;

the first device electronic currency comprises a first device offline electronic currency and
30 a first device in-transit electronic currency;

the wallet information further comprises a second transaction record; wherein the second transaction record comprises second transaction data at least comprising: second transaction information and second signature information obtained by signing the second transaction information by a second device; and the second transaction information comprises second device offline account information, the first device offline account information, second transaction time and a second transaction amount;

said performing the verification operation by the second security control module further comprises: verifying, by the second security control module, the second signature information by using a public key of the second device; and

the passing of the verification by the second security control module further comprises the second security control module verifying and passing the second signature information by using the public key of the second device.

5. The method according to claim 4, wherein the first transaction information further comprises the second transaction record.

6. The method according to claim 1, wherein the collection information further comprises the first transaction amount received by the second security control module through a keyboard module.

7. A computer-readable storage medium, comprising computer instructions that, when executed on a processor, perform the offline electronic currency collection method of any one of claims 1-6.