

CLAIMS

What is claimed is:

1. An offline payment authorization method, applied to a server, wherein the method comprises:

obtaining wallet account information, a current account balance, and current credit information of a target electronic wallet account when it is detected that a current state of the target electronic wallet account satisfies a predetermined certificate delivery condition;

determining a corresponding offline payment limit based on the current account balance and the current credit information;

signing summary information by using a server private key to obtain an electronic wallet signature, wherein the summary information comprises the wallet account information, the offline payment limit, an issuance time, and validity duration;

generating a user certificate based on the summary information and the electronic wallet signature; and

delivering the user certificate to a terminal device that has the target electronic wallet account so that an offline account corresponding to the target electronic wallet account can make offline payment within the offline payment limit based on the user certificate.

2. The method according to claim 1, wherein the predetermined certificate delivery condition comprises at least one of the following conditions: an obtained user certificate of the target electronic wallet account expires, and the terminal device is connected to the internet;

it is the first time period before the obtained user certificate expires, and the terminal device is connected to the internet;

it is the second time period before the obtained user certificate expires, and a mobile data usage state of the terminal device satisfies a predetermined idle condition;

a change of the current account balance and/or the current credit information of the target electronic wallet account satisfies a specific condition; and

the target electronic wallet account has not obtained a user certificate, and the mobile data usage state of the terminal device satisfies a predetermined idle condition.

3. The method according to claim 1, wherein the wallet account information is a

hash value of a wallet account ID and wallet account name information that are corresponding to the target electronic wallet account.

4. The method according to claim 1, wherein the current credit information comprises at least one of the following information: a current credit value and a current available credit limit.

5. The method according to claim 1, wherein the terminal device is provided with a trusted execution environment TEE, and

the delivering the user certificate to a terminal device that has the target electronic wallet account comprises:

delivering the user certificate to the TEE of the terminal device so that the terminal device stores the user certificate in the TEE.

6. The method according to claim 1, wherein the determining a corresponding offline payment limit based on the current account balance and the current credit information comprises:

determining a current score of the target electronic wallet account based on the current account balance, the current credit information, and weights of the current account balance and the current credit information; and

determining the offline payment limit corresponding to the target electronic wallet account based on the current score.

7. The method according to claim 6, wherein the determining the offline payment limit corresponding to the target electronic wallet account based on the current score comprises:

determining a current limit level corresponding to the current score based on a predetermined first mapping relationship between an account score and a limit level; and

determining a limit value corresponding to the current limit level as the offline payment limit based on a predetermined second mapping relationship between a limit level and a limit value.

8. The method according to any one of claims 1 to 7, further comprising:

obtaining an offline bill sent by the terminal device, wherein the offline bill is a bill generated by the offline account after offline payment, and comprises at least a corresponding transaction amount and the wallet account information;

deducting a corresponding amount from the target electronic wallet account based on the transaction amount and the wallet account information; and

sending limit recovery information to the terminal device so that a current upper limit for offline payment of the offline account is restored to the offline payment limit.

9. The method according to claim 8, wherein the offline bill further comprises corresponding merchant account information and a merchant signature, and the merchant signature is obtained by signing the merchant account information and the transaction amount by using a merchant private key; and

the deducting a corresponding amount from the target electronic wallet account based on the transaction amount and the wallet account information comprises:

verifying the offline bill by using a merchant public key corresponding to the merchant private key; and

deducting the corresponding amount from the target electronic wallet account based on the transaction amount and the wallet account information if the verification succeeds.

10. An offline payment method, applied to a terminal device, wherein the terminal device stores a user certificate delivered by a server, the user certificate comprises at least wallet account information of an electronic wallet account corresponding to the terminal device, an offline payment limit, an issuance time, a validity duration, and an electronic wallet signature, and the method comprises:

when an offline payment instruction is received, determining whether a current transaction amount carried in the offline payment instruction is not greater than a current upper limit for offline payment, wherein the current upper limit for offline payment is determined based on the offline payment limit and a historical offline transaction amount;

providing the user certificate to a payment collection device corresponding to the offline payment instruction if it is determined that the current transaction amount is not greater than the current upper limit for offline payment;

obtaining transaction confirmation information provided by the payment collection device, wherein the transaction confirmation information is sent when the payment collection device determines, based on the electronic wallet signature, that the user certificate is valid; and

generating an offline bill based on the transaction confirmation information.

11. The method according to claim 10, wherein the terminal device comprises a trusted execution environment TEE, the user certificate is stored in the TEE, and the method is executed in the TEE.

12. The method according to claim 10, further comprising:

determining whether the user certificate is valid based on a receiving time of the offline payment instruction and the issuance time and validity duration of the user certificate; and

providing the user certificate to the payment collection device when it is determined that the user certificate is valid.

13. The method according to claim 10, further comprising:

calculating a difference between the current upper limit for offline payment and the current transaction amount; and

determining the difference as a new current upper limit for offline payment.

14. The method according to claim 10, further comprising:

sending the offline bill to the server when the terminal device is connected to the internet so that the server performs settlement based on the offline bill.

15. The method according to claim 10, wherein the obtaining transaction confirmation information provided by the payment collection device comprises:

obtaining, in a short-range transmission method, the transaction confirmation information provided by the payment collection device.

16. The method according to claim 10, wherein the transaction confirmation information comprises merchant account information of the merchant, the current transaction amount, and a merchant signature, and the merchant signature is obtained by signing the merchant account information and the current transaction amount by using a merchant private key; and

the generating an offline bill based on the transaction confirmation information comprises:

verifying the transaction confirmation information based on a merchant public key corresponding to the merchant private key; and

generating the offline bill based on the merchant account information, the current transaction amount, and the wallet account information if the verification succeeds.

17. A payment collection method for an offline device, applied to a payment collection device, wherein the method comprises:

obtaining a user certificate provided by an offline terminal device, wherein the user certificate is delivered by a server, and comprises wallet account information of an electronic wallet account corresponding to the terminal device, an offline payment limit, an issuance time and validity duration of the user certificate, and an electronic wallet

signature;

verifying the electronic wallet signature by using a public key of the server;

if the verification succeeds, determining whether the user certificate is valid based on a transaction time of the current transaction, the issuance time, and the validity duration;

generating transaction confirmation information corresponding to the current transaction when it is determined that the user certificate is valid; and

providing the transaction confirmation information to the terminal device so that the terminal device generates a corresponding offline bill based on the transaction confirmation information.

18. The method according to claim 17, wherein the transaction confirmation information comprises at least merchant account information of the merchant, a current transaction amount, and a merchant signature, and the merchant signature is obtained by signing the merchant account information and the current transaction amount by using a merchant private key.

19. The method according to claim 17, wherein the providing the transaction confirmation information to the terminal device comprises:

providing the transaction confirmation information to the terminal device in a short-range transmission method.

20. The method according to claim 17, further comprising:

generating transaction failure information when it is determined that the user certificate is invalid; and

providing the transaction failure information to the terminal device.

21. An offline payment authorization apparatus, applied to a server, wherein the apparatus comprises:

a first acquisition module, configured to obtain wallet account information, a current account balance, and current credit information of a target electronic wallet account when it is detected that a current state of the target electronic wallet account satisfies a predetermined certificate delivery condition;

a first determining module, configured to determine a corresponding offline payment limit based on the current account balance and the current credit information;

a first signing module, configured to sign summary information by using a server private key to obtain an electronic wallet signature, wherein the summary information comprises the wallet account information, the offline payment limit, an issuance time,

and validity duration;

a first generation module, configured to generate a user certificate based on the summary information and the electronic wallet signature; and

a first sending module, configured to deliver the user certificate to a terminal device that has the target electronic wallet account so that an offline account corresponding to the target electronic wallet account can make offline payment within the offline payment limit based on the user certificate.

22. An offline payment apparatus, applied to a terminal device, wherein the terminal device stores a user certificate delivered by a server, the user certificate comprises at least wallet account information of an electronic wallet account corresponding to the terminal device, an offline payment limit, an issuance time, a validity duration, and an electronic wallet signature, and the apparatus comprises:

a first judgment module, configured to: when an offline payment instruction is received, determine whether a current transaction amount carried in the offline payment instruction is not greater than a current upper limit for offline payment, wherein the current upper limit for offline payment is determined based on the offline payment limit and a historical offline transaction amount;

a first provision module, configured to provide the user certificate to a payment collection device corresponding to the offline payment instruction if it is determined that the current transaction amount is not greater than the current upper limit for offline payment;

a second acquisition module, configured to obtain transaction confirmation information provided by the payment collection device, wherein the transaction confirmation information is sent when the payment collection device determines, based on the electronic wallet signature, that the user certificate is valid; and

a second generation module, configured to generate an offline bill based on the transaction confirmation information.

23. A payment collection apparatus for an offline device, applied to a payment collection device, wherein the apparatus comprises:

a third acquisition module, configured to obtain a user certificate provided by an offline terminal device, wherein the user certificate is delivered by a server, and comprises wallet account information of an electronic wallet account corresponding to the terminal device, an offline payment limit, an issuance time and validity duration of the user certificate, and an electronic wallet signature;

a first verification module, configured to verify the electronic wallet signature by using a public key of the server;

a second judgment module, configured to: if the verification succeeds, determine whether the user certificate is valid based on a transaction time of the current transaction, the issuance time, and the validity duration;

a third generation module, configured to generate transaction confirmation information corresponding to the current transaction when it is determined that the user certificate is valid; and

a second provision module, configured to provide the transaction confirmation information to the terminal device so that the terminal device generates a corresponding offline bill based on the transaction confirmation information.

24. A computing device, comprising a storage and a processor, wherein the storage stores executable code, and when executing the executable code, the processor implements the method according to any one of claims 1 to 9, claims 10 to 16, or claims 17 to 20.