PAYMENT CARD BINDING METHOD, TRUST EVALUATION METHOD, APPARATUS, AND ELECTRONIC DEVICE

TECHNICAL FIELD

[0001] The present application relates to the field of computer software technologies, and in particular, to a payment card binding method, a trust evaluation method, an apparatus, and an electronic device.

BACKGROUND

[0002] When a user uses a digital wallet for payment, the digital wallet often needs to be bound to more than one payment card.

[0003] When the user binds a new payment card to the digital wallet, a verification method that is mostly used at present is 3-D Secure and Micro Charge.

[0004] 3-D Secure: based on a 3-D model authentication process, the 3-D includes an acquirer domain, an issuer domain, and an interoperability domain.

[0005] Micro Charge: The digital wallet makes a random small payment to a credit card of the user. Please check if the user knows the amount for authentication.

[0006] However, verification manners of the two verification methods are relatively complex, and a payment failure rate (a probability of giving up card binding and payment) of the user is relatively high. According to statistics, payment failure rates of both solutions are more than 30%-40%.

SUMMARY

[0007] Embodiments of the present application are intended to provide a payment card binding method, a trust evaluation method, an apparatus, and an electronic device, so as to simplify a process of binding a new card and reduce a payment risk.

[0008] In order to resolve the foregoing technical problem, embodiments of the present application are implemented in a manner below.

[0009] In a first aspect, a payment card binding method is provided, including:

[0010] sending, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem;

[0011] when the payment is successful, determining, based on at least one of device

data, environment data, and account data of the payment client, trust evaluation parameters corresponding to a payment card and a payment client account; and

[0012] performing, based on the trust evaluation parameters, binding configuration on the payment client account and the payment card, the trust evaluation parameters being used to determine payment limit restrictions.

[0013] In a second aspect, a payment card trust evaluation method is provided, including:

[0014] receiving a trust evaluation parameter acquisition request for a payment card sent by a payment server, where the trust evaluation parameter acquisition request is sent by the payment server when receiving a payment success indication fed back by a payment ecosystem; and

[0015] sending, to the payment server based on the trust evaluation parameter acquisition request, trust evaluation parameters corresponding to the payment card and the payment client account, where the trust evaluation parameters are used by the payment server to bind the payment client account to the payment card and determine payment limit restrictions.

[0016] In a third aspect, a payment card binding apparatus is provided, including:

[0017] a payment unit configured to send, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem;

[0018] a determining unit configured to: when the payment is successful, determine, based on at least one of device data, environment data, and account data of the payment client, trust evaluation parameters corresponding to a payment card and a payment client account; and

[0019] a binding unit configured to perform, based on the trust evaluation parameters, binding configuration on the payment client account and the payment card, the trust evaluation parameters being used to determine payment limit restrictions.

[0020] In a fourth aspect, a payment card trust evaluation apparatus is provided, including:

[0021] a receiving unit configured to receive a trust evaluation parameter acquisition request for a payment card sent by a payment server, where the trust evaluation parameter acquisition request is sent by the payment server when receiving a payment success indication fed back by a payment ecosystem; and

[0022] a sending unit configured to send, to the payment server based on the trust evaluation parameter acquisition request, trust evaluation parameters corresponding to the

payment card and the payment client account, where the trust evaluation parameter is used by the payment server to bind the payment client account to the payment card and determine payment limit restrictions.

[0023] In a fifth aspect, an electronic device is provided, including:

[0024] a processor; and

[0025] a memory configured to store a computer executable instruction that, when executed, causes the processor to perform the following operations:

[0026] sending, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem;

[0027] when the payment is successful, determining, based on at least one of device data, environment data, and account data of the payment client, trust evaluation parameters corresponding to a payment card and a payment client account; and

[0028] performing, based on the trust evaluation parameters, binding configuration on the payment client account and the payment card, the trust evaluation parameters being used to determine payment limit restrictions.

[0029] In a sixth aspect, a computer-readable storage medium is provided, the computer-readable storage medium storing one or more programs that, when executed by an electronic device including a plurality of application programs, cause the electronic device to perform the following operations:

[0030] sending, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem;

[0031] when the payment is successful, determining, based on at least one of device data, environment data, and account data of the payment client, trust evaluation parameters corresponding to a payment card and a payment client account; and

[0032] performing, based on the trust evaluation parameters, binding configuration on the payment client account and the payment card, the trust evaluation parameters being used to determine payment limit restrictions.

[0033] In a seventh aspect, an electronic device is provided, including:

[0034] a processor; and

[0035] a memory configured to store a computer executable instruction that, when executed, causes the processor to perform the following operations:

[0036] receiving a trust evaluation parameter acquisition request for a payment card sent by a payment server, where the trust evaluation parameter acquisition request is sent by the payment server when receiving a payment success indication fed back by a payment

ecosystem; and

[0037] sending, to the payment server based on the trust evaluation parameter acquisition request, trust evaluation parameters corresponding to the payment card and the payment client account, where the trust evaluation parameters are used by the payment server to bind the payment client account to the payment card and determine payment limit restrictions.

[0038] In an eighth aspect, a computer-readable storage medium is provided, the computer-readable storage medium storing one or more programs that, when executed by an electronic device including a plurality of application programs, cause the electronic device to perform the following operations:

[0039] receiving a trust evaluation parameter acquisition request for a payment card sent by a payment server, where the trust evaluation parameter acquisition request is sent by the payment server when receiving a payment success indication fed back by a payment ecosystem; and

[0040] sending, to the payment server based on the trust evaluation parameter acquisition request, trust evaluation parameters corresponding to the payment card and the payment client account, where the trust evaluation parameters are used by the payment server to bind the payment client account to the payment card and determine payment limit restrictions.

[0041] It may be seen from the technical solutions provided by the foregoing embodiments of the present application that the solutions of the embodiments of the present application have at least one of the following technical effects:

[0042] In a first aspect, validity of the payment card is determined by initiating a payment to the payment card to be bound to the payment client, and based on at least one of the account data, the device data, and the environment data of the payment client, the trust evaluation parameter of the payment card is determined. Therefore, the binding process may be simplified, and a payment risk after the new card is bound is reduced.

[0043] In a second aspect, by receiving a trust evaluation parameter acquisition request sent by the payment server when the payment card is valid, the trust evaluation parameters are fed back to the payment server, for the payment server to bind the payment card based on the trust evaluation parameters. Therefore, a new card binding process is simplified, and a payment risk after the new card is bound is reduced.

BRIEF DESCRIPTION OF THE DRAWINGS

[0044] To describe the technical solutions in the embodiments of the present application or in the existing technologies more clearly, the following briefly introduces the accompanying drawings required for describing the embodiments or the existing technologies. Apparently, the accompanying drawings in the following description show merely some embodiments of the present application, and a person of ordinary skill in the art may still derive other drawings from these accompanying drawings without creative efforts.

[0045] FIG. 1 is a flowchart of a payment card binding method, according to an embodiment of the present application.

[0046] FIG. 2 is a flowchart of interaction of payment card binding with payment card trust evaluation, according to an embodiment of the present application.

[0047] FIG. 3 is a flowchart of a payment card trust evaluation method, according to an embodiment of the present application.

[0048] FIG. 4 is a schematic structural diagram of an electronic device, according to an embodiment of the present application.

[0049] FIG. 5 is a schematic structural diagram of a payment card binding apparatus, according to an embodiment of the present application.

[0050] FIG. 6 is a schematic structural diagram of an electronic device, according to an embodiment of the present application.

[0051] FIG. 7 is a schematic structural diagram of a payment card trust evaluation apparatus, according to an embodiment of the present application.

DETAILED DESCRIPTION OF THE INVENTION

[0052] Embodiments of the present application provide a payment card binding method, a trust evaluation method, an apparatus, and an electronic device.

[0053] To enable a person skilled in the art to better understand the technical solutions of the present application, the technical solutions of the embodiments of the present application will be described clearly and thoroughly below with reference to the accompanying drawings of the embodiments of the present application. Apparently, the described embodiments are merely some rather than all of the embodiments of the present application. All other embodiments obtained by a person of ordinary skill in the art based on the embodiments of the present application without creative efforts shall fall within the protection scope of the present application.

[0054] FIG. 1 is a flowchart of a payment card binding method, according to an

embodiment of the present application. The method in FIG. 1 may be applied to a payment server, such as an electronic wallet server, and an Alipay system server, etc. The method in FIG. 1 may include below.

[0055] S110. Send, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem.

[0056] It should be understood that, in an embodiment of the present application, the payment client may be an electronic wallet client and so on. In a payment client account, a user may bind a new payment card, such as a credit card, a debit card, and a Visa card, etc. In this case, the user may send a payment card binding request to a payment server to perform a payment card binding process.

[0057] It should be understood that, in the embodiment of the present application, the payment ecosystem refers to a payment service provider, including an acquirer, a card organization, and a card issuer (a card issuing bank) etc. It should be understood that the acquirer may provide payment and clearing services to a merchant and forward a transaction to the card connection organization. The card organization may transfer the transaction to the card issuer, and is responsible for settlement among the acquirer and the card issuer. The card issuer is responsible for providing a card product to a consumer, such as a bank card applied at a bank, etc. Definitely, it should be understood that, the transaction process between payment ecosystems is not limited in the embodiment of the present application, and other possible implementation for the payment ecosystems are not excluded.

[0058] After receiving the payment card binding request sent by the payment client, the payment server may send a first payment request to the payment ecosystem to verify validity of the payment card.

[0059] It should be understood that when sending the first payment request, the payment server may initiate a micro-payment request to verify the validity of the payment card. The payment server may initiate a payment request (deduction request) to the payment ecosystem through a deduction transaction message. If the payment ecosystem responds to the payment request and feeds back a payment success result, it means that the payment card is valid. On the contrary, if the payment ecosystem feeds back a payment failure result, it means that the payment card is invalid. In this case, subsequent steps are not performed any more.

[0060] It should be understood that an amount in the payment request may be fixed or random. For example, deduction of 0.13 Yuan may be randomly sent, and so on.

[0061] S120. When the payment is successful, determine, based on at least one of

device data, environment data, and account data of the payment client, trust evaluation parameters corresponding to the payment card and a payment client account.

[0062] It should be understood that the device data of the payment client may include: for example, a device ID and a device MAC address, etc.

[0063] Based on the device data of the payment client, a device trust level may be determined.

[0064] For example, if a device is a device commonly used by the payment client account, the device trust level and the corresponding trust evaluation parameter are higher. If the device is a device used by the payment client account for the first time, the device trust level and the corresponding trust evaluation parameter are lower. For another example, if the device has a fraud history, the device trust level and the corresponding trust evaluation parameter are lower.

[0065] The environment data of the payment client may include: for example, a name of a WIFI connected to a terminal device at which the payment client is located, a MAC address of the WIFI, a geographic location (latitude and longitude information) of the device, and an IP address field.

[0066] Based on the environment data of the payment client, an environment trust level may also be determined.

[0067] Similarly, if the environment data indicates that the user is not in a resident location, such as being abroad, the environment trust level is lower, and the corresponding trust evaluation parameter is lower.

[0068] The account data of the payment client may include: for example, a payment client account ID, registration time, a customer name, a gender, an address, an age, a funding channel, and customer data modification history, etc.

[0069] Based on the account data of the payment client, an account trust level may also be determined.

[0070] For example, if an age corresponding to the payment client account is between 30 and 40, the account trust level is higher. If the age corresponding to the payment client account is between 8 and 12, the account trust level is lower. For another example, if the payment client account has a fraud history, the account trust level is lower, and so on.

[0071] Based on one or more of the device data, the environment data, and the account data, the trust evaluation parameters corresponding to the payment card and the payment client account may be determined.

[0072] S130. Perform, based on the trust evaluation parameters, binding configuration

on the payment client account and the payment card.

[0073] The trust evaluation parameter is used to determine payment limit restrictions.

[0074] After the trust evaluation parameters are determined, the payment client account may be bound to the payment card based on the trust evaluation parameters.

[0075] Optionally, the trust evaluation parameters include at least one of the following: a payment card trust level and payment restrictions associated with the payment card trust level. It should be understood that in the process of binding a new card, a risk control system may feed back to the payment server at least one of a new card trust level (NCTL) or a payment restriction corresponding to the NCTL.

[0076] Correspondingly, step S130 may be implemented in a manner below.

[0077] When the payment client account is bound to the payment card, based on the trust evaluation parameters, at least one of a trust level and payment restrictions of the payment card in the payment client account is set.

[0078] For example, it is assumed that the risk control system has five NCTL levels of 0, 1, 2, 3, and 4, the NCTL level and the trust level are higher and the risk is lower. It is further assumed that the payment restrictions corresponding to all of the NCTL levels are 0 Yuan, 100 Yuan, 500 Yuan, 1000 Yuan, and 2000 Yuan, respectively. When the risk control system determines that the NCTL level is 1 based on the device data of the payment client, the environment data of the payment client, a payment card identifier, and the account data of the payment client, etc., the level 1 may be fed back to the payment server, or a payment restriction of 100 Yuan may be fed back to the payment server, or information about both the level 1 and 100 Yuan are fed back to the payment server. Definitely, it should be understood that in this example, if it is determined that the NCTL is a level 0, it means that a confidence level of the payment card is extremely low, and the payment client account bound to the payment card has a higher risk.

[0079] In the embodiment of the present application, the validity of the payment card is determined by initiating a payment to the payment card to be bound to the payment client, and based on at least one of the account data, the device data, and the environment data of the payment client, the trust evaluation parameter of the payment card is determined. Therefore, the binding process is simplified, and a payment risk after the new card is bound is reduced.

[0080] Optionally, as an embodiment, the payment server may include a risk control module for determining, based on at least one of the device data, the environment data, and the account data of the payment client, the trust evaluation parameters corresponding to the payment card and the payment client account.

[0081] Optionally, as another embodiment, the payment server has no risk control module. In this case, the step S120 may be implemented as a manner below:

[0082] a trust evaluation parameter acquisition request about the payment card and the payment client account is sent to the risk control system, the trust evaluation parameter acquisition request including at least one of the device data, the environment data, and the account data of the payment client, and the payment card identifier; and

[0083] a trust evaluation parameter fed back by the risk control system is received based on the trust evaluation parameter acquisition request.

[0084] Optionally, after the step S130, the method may further include:

[0085] a payment amount in the first payment request is recharged into the payment client account.

[0086] Optionally, after the step S130, the method may further include:

[0087] a second payment request about the payment card under the payment client account is sent to the payment ecosystem; and

[0088] a trust evaluation is performed on the second payment request to determine whether to allow the second payment request.

[0089] It should be understood that when the payment server receives the payment request about the payment card sent by the payment client account, the payment request may be sent to the risk control system to perform risk verification on the payment request. The risk control system may determine whether to allow the payment based on payment refusal data, transaction data, and trust level data of the payment card, as well as a payment limit carried in the payment request. The risk verification of the payment request by the risk control system may further reduce the payment risk after the payment card is bound.

[0090] Further, the method further includes: if the second payment request is not allowed, an offsetting is performed on the payment ecosystem based on the second payment request.

[0091] Definitely, it should be understood that, in the step of performing a trust evaluation on the second payment request to determine whether to allow the second payment request, when the payment server has no risk control module, the step may be implemented in a manner below:

[0092] a verification request for the second payment request is sent to the risk control system, the verification request including the payment card identifier, the payment client account, and the payment amount of the second payment request; and

[0093] a response from the risk control system to the verification request is received,

the response being determined by the risk control system based on the trust evaluation parameters corresponding to the payment card and the payment client account, and the payment amount of the second payment request.

[0094] Optionally, the response may further carry the trust evaluation parameters adjusted by the risk control system. The method further includes:

[0095] based on the adjusted trust evaluation parameters, binding parameters of the binding configuration for the payment client account and the payment card are reset.

[0096] Correspondingly, if the payment server has the risk control module, after the step S130, the method may further include:

[0097] Based on the payment refusal data, transaction data, and trust evaluation parameters after the payment card is bound to the payment client account, the trust evaluation parameters corresponding to the payment card and the payment client account are adjusted.

[0098] When the trust evaluation parameters are adjusted based on the payment refusal data, transaction data, and the current trust evaluation parameters, the payment restrictions may be adjusted with an increase in the number of transaction times of the bound payment card, for the payment restrictions to match the payment client account, payment card, device, environment and other factors.

[0099] Next, the method in the embodiment of the present application is further described in combination with a specific embodiment.

[0100] FIG. 2 is a flowchart of interaction of payment card binding with payment card trust evaluation, according to an embodiment of the present application. In the embodiment shown in FIG. 2, information interaction among four parties including a wallet client, a wallet server, a payment ecosystem, and a risk control system may be included.

[0101] The wallet client, that is, the payment client of the embodiment shown in FIG. 1, may be configured to initiate a new card binding request.

[0102] The wallet server, that is, the payment server in the embodiment shown in FIG. 1, may respond to the new card binding request of the wallet client and perform operations related to new card binding.

[0103] The payment ecosystem, that is, the payment ecosystem of the embodiment shown in FIG. 1, is a provider of a payment service. In an embodiment shown in Figure 2, the payment ecosystem may include an acquirer, a card organization, and a card issuer. The acquirer may provide payment and clearing services to a merchant and forward a transaction to the card connection organizations. The card organization may transfer the transaction to the card issuer, and is responsible for settlement among the acquirer and the card issuer. The

card issuer is responsible for providing a card product to a consumer, such as a bank card applied at a bank, etc.

[0104] The risk control system, that is, the risk control system of the embodiment shown in FIG. 1, is configured to calculate and update of a wallet account trust level, a device trust level, and an environment trust level of the NCTL in real time, to update NCTL and NCTL-associated expenditure restrictions, which are used as a response from the wallet server. The risk control system may provide an API interface, and the wallet server may acquire, through the API interface, the NCTL corresponding to the new card and the wallet client account and/or payment restrictions corresponding to the NCTL.

[0105] Next, a solution process is described in detail.

[0106] Step 1. A wallet client sends a new card binding request to a wallet server.

[0107] It should be understood that when the wallet client sends the new card binding request, an account identifier of the wallet client and related parameters of the to-be-bound payment card may be sent to the wallet server.

[0108] Payment card related parameters are, for example, a payment card identifier and a payment card password. Definitely, the payment card related parameters may further include at least one of a verification code of the payment card, a mobile phone number bound to the payment card at a card issuing bank, a user identity of the payment card, and other pieces of information.

[0109] Definitely, it should be understood that the wallet client may further send other pieces of account data of the wallet client to the wallet server.

[0110] The wallet client may further send device data to the wallet client. The device data is, for example, a device identifier of the terminal device at which the wallet client is located and a MAC address, etc.

[0111] The wallet client may further send environment data to the wallet client. The environment data is, for example, a name of a WIFI connected to a terminal device at which the payment client is located, a MAC address of the WIFI, a geographic location (latitude and longitude information) of the device, and an IP address field. The geographic location of the device is obtained, for example, through a location based service (LBS) of the terminal device.

[0112] Step 2. The wallet server sends a payment request to the payment ecosystem.

[0113] Based on the new card binding request of the wallet client, the wallet server may send the payment request to the payment ecosystem to verify validity of a new card.

[0114] In particular, for example, the wallet server may send a deduction request to

the payment ecosystem through a deduction transaction message to verify the validity of the new card. For example, the payment server may initiate a random micro-payment amount, such as 0.13 Yuan, and so on.

[0115] According to the deduction transaction message, the payment ecosystem may return a response to a deduction success or a deduction failure. Referring to existing technologies for a specific processing manner thereof, and details thereof are not described in the embodiment of the present application.

[0116] Step 3. The wallet server sends a trust evaluation parameter acquisition request to the risk control system.

[0117] In the embodiment shown in FIG. 2, the wallet server may send the trust evaluation parameter acquisition request to the risk control system by invoking an NCTL Risk Service API to acquire trust evaluation parameters corresponding to the new card and the wallet client account.

[0118] As shown in FIG. 2, as an input to the NCTL Risk Service API, a new card identifier, a wallet client account data, device data, and environment data may be included.

[0119] Step 4. The risk control system calculates trust evaluation parameters.

[0120] The risk control system may obtain an account trust level (ATL) through calculation based on the wallet client account data.

[0121] The risk control system may obtain a device trust level (DTL) through calculation based on the device data.

[0122] The risk control system may obtain an environment trust level (ETL) through calculation based on the environment data.

[0123] ATL, DTL and ETL may be obtained through calculation based on corresponding trust level calculation models.

[0124] Based on the ATL, DTL and ETL, a corresponding NCTL may be obtained for the risk control system. A manner of calculating NCTL may also be obtained based on an NCTL model.

[0125] A training manner of the foregoing model may be obtained based on corresponding training data, which is not limited in the embodiment of the present application.

[0126] Definitely, it should be understood that parameters for determining the NCTL may include only one or more of the ATL, DTL, and ETL, and may further include parameters except the ATL, DTL, and ETL, which are not limited in the embodiment of the present application.

[0127] In addition, based on the NCTL, the risk control system may further determine a payment limit corresponding to the NCTL.

[0128] Step 5. The risk control system feeds back the trust evaluation parameters.

[0129] As shown in Figure 2, the risk control system may feed back to the wallet server NCTL and payment restrictions corresponding to the NCTL. Definitely, it should be understood that the risk control system may also feed only one of the NCTL and the payment restrictions back to the wallet server.

[0130] Step 6. The wallet server binds the payment card and a wallet client account.

[0131] Based on the trust evaluation parameters fed back by the risk control system, the wallet server may bind the payment card to wallet client account and set corresponding binding parameters of the binding configuration, such as the NCTL, payment restrictions, and so on.

[0132] So far, the binding process of the payment card is completed.

[0133] In addition, it should be understood that in a subsequent payment process, referring to the solution shown in FIG. 2, the payment server may also initiate a payment request to the payment ecosystem, and then send the payment request to the risk control system for verification. The risk control system may determine whether to allow the payment request based on the current NCTL and payment restrictions of the payment card and wallet client account. If no, offsetting is initiated to the payment ecosystem.

[0134] Definitely, it should be understood that the risk control system may further adjust the NCTL corresponding to the payment card and the wallet client account based on payment refusal records, transaction records, and the current NCTL generated after the payment card is bound to the wallet client account.

[0135] In addition, it should be understood that the payment server and the risk control system in the foregoing embodiments may also be combined into one system.

[0136] FIG. 3 is a flowchart of a trust evaluation method for a payment card. The method of FIG. 3 is implemented by a risk control system. The method may include below.

[0137] S310. Receive a trust evaluation parameter acquisition request for a payment card sent by a payment server.

[0138] The trust evaluation parameter acquisition request is sent by the payment server when receiving payment success indication fed back by a payment ecosystem.

[0139] S320. Send, to the payment server based on the trust evaluation parameter acquisition request, trust evaluation parameters corresponding to the payment card and the payment client account.

[0140] The trust evaluation parameters are used by the payment server to bind the payment client account and the payment card, and determine payment limit restrictions.

[0141] In an embodiment of the present application, by receiving a trust evaluation parameter acquisition request sent by the payment server when the payment card is valid, the trust evaluation parameters are fed back to the payment server, for the payment server to bind the payment card based on the trust evaluation parameters. Therefore, a new card binding process is simplified, and a payment risk after the new card is bound is reduced.

[0142] Optionally, the trust evaluation parameter acquisition request includes: at least one of device data, environment data, and account data of the payment client, and a payment card identifier.

[0143] Optionally, step S320 may be specifically implemented below:

[0144] a device trust level is determined based on the device data of the payment client;

[0145] an environment trust level is determined based on the environment data of the payment client;

[0146] an account trust level is determined based on the account data of the payment client; and

[0147] the trust evaluation parameters are determined based on the device trust level, the environment trust level, and the account trust level.

[0148] Definitely, it should be understood that the trust evaluation parameters may also be determined based on one or two of the device trust level, the environment trust level, and the account trust level.

[0149] Optionally, the trust evaluation parameters include at least one of the following: a payment card trust level and payment restrictions associated with the payment card trust level.

[0150] Optionally, the method further includes:

[0151] Based on the payment refusal data, transaction data, and trust evaluation parameters after the payment card is bound to the payment client account, the trust evaluation parameters corresponding to the payment card and the payment client account are adjusted.

[0152] Optionally, the method further includes:

[0153] a verification request sent by the payment server is received, the verification request being used to request to perform verification to determine whether to allow a payment request for the payment card under the payment client account; and

[0154] a response to the verification request is fed back to the payment server based

on current trust evaluation parameters of the payment card and the payment client account.

[0155] For specific implementation of the embodiment shown in FIG. 3, reference may be made to the method performed by the risk control system in the embodiments shown in FIG. 1 and FIG. 2, and details thereof are not described in the embodiment of the present application.

[0156] Embodiments of the present specification are described above. Other embodiments fall within the scope of the appended claims. In some embodiments, the actions or steps recorded in the claims may be performed in sequences different from those in the embodiments and an expected result may still be achieved. In addition, the processes depicted in the accompanying drawings do not necessarily require specific sequences or consecutive sequences to achieve an expected result. In some implementations, multitasking and parallel processing may be feasible or beneficial.

[0157] FIG. 4 is a schematic structural diagram of an electronic device according to an embodiment of the present application. Referring to FIG. 4, at the hardware level, the electronic device includes a processor, and optionally, includes an internal bus, a network interface, and a memory. The memory may include a memory, for example, a random access memory (RAM), or may further include a non-volatile memory, for example, at least one magnetic disk memory. Certainly, the electronic device may further include hardware required for other services.

[0158] The processor, the network interface, and the memory may be connected to each other through the internal bus. The internal bus may be an industry standard architecture (ISA) bus, a peripheral component interconnect (PCI) bus, or an extended industry standard architecture (EISA) bus. The bus may be classified into an address bus, a data bus, a control bus, and the like. For ease of illustration, in FIG. 4, the bus is represented by using only one double-sided arrow. This, however, does not indicate that there is only one bus or only one type of bus.

[0159] The memory is configured to store a program. Specifically, the program may include program code, where the program code includes a computer operation instruction. The memory may include an internal memory and a non-volatile memory, and provide instructions and data to the processor.

[0160] The processor reads a corresponding computer program from the non-volatile memory into the memory and then executes the computer program, to form a payment card binding apparatus at the logic level. The processor executes the program stored in the memory and is specifically configured to perform the following operations:

[0161] sending, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem;

[0162] when the payment is successful, determining, based on at least one of device data, environment data, and account data of the payment client, trust evaluation parameters corresponding to a payment card and a payment client account; and

[0163] performing, based on the trust evaluation parameters, binding configuration on the payment client account and the payment card, the trust evaluation parameters being used to determine payment limit restrictions.

[0164] The method performed by the payment card binding apparatus disclosed in the embodiment shown in FIG. 1 of the present application may be applied to a processor, or may be implemented by a processor. The processor may be an integrated circuit chip and has a signal processing capability. In an implementation process, steps of the foregoing method may be implemented by using a hardware integrated logic circuit in the processor or instructions in a form of software. The processor may be a general processor, including a central processing unit (CPU), a network processor (NP), and the like; or may further be a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA), or another programmable logical device, discrete gate or transistor logical device, or discrete hardware component. It may implement or perform the methods, the steps, and logical block diagrams that are disclosed in the embodiments of the present application. The general-purpose processor may be a microprocessor, or the processor may be any conventional processor or the like. Steps of the methods disclosed with reference to the embodiments of the present application may be directly performed and completed by using a hardware decoding processor, or may be performed and completed by using a combination of hardware and a software module in the decoding processor. The software module may be located in a mature storage medium in the art, such as a RAM, a flash memory, a ROM, a programmable ROM, an electrically erasable programmable memory, or a register. The storage medium is located in the memory, and the processor reads information in the memory and completes the steps in the foregoing methods in combination with hardware of the processor.

[0165] The electronic device may also perform the method of FIG. 1 and implement the functions of the payment server or the wallet server in the embodiments shown in FIG. 1 and FIG. 2, and details are not described again in the embodiment of the present application.

[0166] Definitely, in addition to a software implementation, the electronic device in the present application does not exclude other implementations, for example, a logic device

or a combination of software and hardware. In other words, an entity executing the following processing procedure is not limited to the logic units, and may also be hardware or logic devices.

[0167] An embodiment of the present application further provides a computer readable storage medium. The computer readable storage medium stores one or more programs, the one or more programs include an instruction, and when the instruction is executed by a portable electronic device including a plurality of applications, the portable electronic device is enabled to perform the method in the embodiment shown in FIG. 1, and specifically perform the following operations:

[0168] sending, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem;

[0169] when the payment is successful, determining, based on at least one of device data, environment data, and account data of the payment client, trust evaluation parameters corresponding to a payment card and a payment client account; and

[0170] performing, based on the trust evaluation parameters, binding configuration on the payment client account and the payment card, the trust evaluation parameters being used to determine payment limit restrictions.

[0171] FIG. 5 is a schematic structural diagram of a payment card binding apparatus, according to an embodiment of the present application. Referring to FIG. 5, in a software implementation, a payment card binding apparatus 500 may include:

[0172] a payment unit 510 configured to send, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem;

[0173] a determining unit 520 configured to, when the payment is successful, determine, based on at least one of device data, environment data, and account data of the payment client, trust evaluation parameters corresponding to a payment card and a payment client account; and

[0174] a binding unit 530 configured to perform, based on the trust evaluation parameters, binding configuration on the payment client account and the payment card, the trust evaluation parameters being used to determine payment limit restrictions.

[0175] In the embodiment of the present application, the validity of the payment card is determined by initiating a payment to the payment card to be bound to the payment client, and based on at least one of the account data, the device data, and the environment data of the payment client, the trust evaluation parameter of the payment card is determined. Therefore, the binding process is simplified, and a payment risk after the new card is bound is reduced.

[0176] Optionally, the determining unit 520 is specifically configured to:

[0177] send, to the risk control system, a trust evaluation parameter acquisition request about the payment card and the payment client account, the trust evaluation parameter acquisition request including at least one of the device data, the environment data, and the account data of the payment client, and the payment card identifier; and

[0178] receive a trust evaluation parameter fed back by the risk control system based on the trust evaluation parameter acquisition request.

[0179] Optionally, the trust evaluation parameter includes at least one of the following: a payment card trust level and payment restrictions associated with the payment card trust level.

[0180] Optionally, the binding unit 530 is specifically configured to: when the payment client account is bound to the payment card, based on the trust evaluation parameters, set at least one of a trust level and payment restrictions of the payment card in the payment client account.

[0181] Optionally, the payment card binding apparatus 500 further includes a recharge unit 540 to recharge a payment amount in the first payment request into the payment client account.

[0182] Optionally, the payment unit 510 further sends, to the payment ecosystem, a second payment request for the payment card under the payment client account.

[0183] The determining unit 520 further performs a trust evaluation on the second payment request to determine whether to allow the second payment request.

[0184] Optionally, the payment card binding apparatus 500 further includes an offsetting unit 550. If the second payment request is not allowed, offsetting is performed to the payment ecosystem based on the second payment request.

[0185] Optionally, the determining unit 520 is further configured to:

[0186] send, to the risk control system, a verification request for the second payment request, the verification request including the payment card identifier, the payment client account, and the payment amount of the second payment request; and

[0187] receive from the risk control system a response to the verification request, the response being determined by the risk control system based on the trust evaluation parameters corresponding to the payment card and the payment client account, and the payment amount of the second payment request.

[0188] Optionally, the response further includes the trust evaluation parameters adjusted by the risk control system. The binding unit 530 is further configured to reset

binding parameters of the binding configuration for the payment client account and the payment card based on the adjusted trust evaluation parameters.

[0189] Optionally, the payment ecosystem includes an acquirer subsystem, a card solution subsystem, and a card issuer subsystem.

[0190] For the payment card binding device, the method in FIG. 1 may be further performed, and the functions of the payment server or wallet server in the embodiments shown in FIG. 1 and FIG. 2 are implemented, and details are not described again in the embodiment of the present application.

[0191] FIG. 6 is a schematic structural diagram of an electronic device according to an embodiment of the present application. Referring to FIG. 6, at the hardware level, the electronic device includes a processor, and optionally, includes an internal bus, a network interface, and a memory. The memory may include a memory, for example, a random access memory (RAM), or may further include a non-volatile memory, for example, at least one magnetic disk memory. Certainly, the electronic device may further include hardware required for other services.

[0192] The processor, the network interface, and the memory may be connected to each other through the internal bus. The internal bus may be an industry standard architecture (ISA) bus, a peripheral component interconnect (PCI) bus, or an extended industry standard architecture (EISA) bus. The bus may be classified into an address bus, a data bus, a control bus, and the like. For ease of illustration, in FIG. 6, the bus is represented by using only one double-sided arrow. This, however, does not indicate that there is only one bus or only one type of bus.

[0193] The memory is configured to store a program. Specifically, the program may include program code, where the program code includes a computer operation instruction. The memory may include an internal memory and a non-volatile memory, and provide instructions and data to the processor.

[0194] The processor reads a corresponding computer program from the non-volatile memory into the memory and then executes the computer program, to form a payment card trust evaluation apparatus at the logic level. The processor executes the program stored in the memory and is specifically configured to perform the following operations:

[0195] receiving a trust evaluation parameter acquisition request for a payment card sent by a payment server, where the trust evaluation parameter acquisition request is sent by the payment server when receiving a payment success indication fed back by a payment ecosystem; and

[0196] sending, to the payment server based on the trust evaluation parameter acquisition request, trust evaluation parameters corresponding to the payment card and the payment client account, where the trust evaluation parameters are used by the payment server to bind the payment client account to the payment card and determine payment limit restrictions.

[0197] The method performed by the payment card trust evaluation apparatus or risk control system disclosed in the embodiment shown in FIG. 3 of the present application may be applied to a processor, or may be implemented by a processor. The processor may be an integrated circuit chip and has a signal processing capability. In an implementation process, steps of the foregoing method may be implemented by using a hardware integrated logic circuit in the processor or instructions in a form of software. The processor may be a general processor, including a central processing unit (CPU), a network processor (NP), and the like; or may further be a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA), or another programmable logical device, discrete gate or transistor logical device, or discrete hardware component. It may implement or perform the methods, the steps, and logical block diagrams that are disclosed in the embodiments of the present application. The general-purpose processor may be a microprocessor, or the processor may be any conventional processor or the like. Steps of the methods disclosed with reference to the embodiments of the present application may be directly performed and completed by using a hardware decoding processor, or may be performed and completed by using a combination of hardware and a software module in the decoding processor. The software module may be located in a mature storage medium in the art, such as a RAM, a flash memory, a ROM, a programmable ROM, an electrically erasable programmable memory, or a register. The storage medium is located in the memory, and the processor reads information in the memory and completes the steps in the foregoing methods in combination with hardware of the processor.

[0198] The electronic device may also perform the method of FIG. 3 and implement the functions of the risk control system in the embodiments shown in FIG. 3 and FIG. 2, and details are not described again in the embodiment of the present application.

[0199] Definitely, in addition to a software implementation, the electronic device in the present application does not exclude other implementations, for example, a logic device or a combination of software and hardware. In other words, an entity executing the following processing procedure is not limited to the logic units, and may also be hardware or logic devices.

[0200] An embodiment of the present application further provides a computer readable storage medium. The computer readable storage medium stores one or more programs, the one or more programs include an instruction, and when the instruction is executed by a portable electronic device including a plurality of applications, the portable electronic device is enabled to perform the method in the embodiment shown in FIG. 3, and specifically perform the following operations:

[0201] receiving a trust evaluation parameter acquisition request for a payment card sent by a payment server, where the trust evaluation parameter acquisition request is sent by the payment server when receiving a payment success indication fed back by a payment ecosystem; and

[0202] sending, to the payment server based on the trust evaluation parameter acquisition request, trust evaluation parameters corresponding to the payment card and the payment client account, where the trust evaluation parameters are used by the payment server to bind the payment client account to the payment card and determine payment limit restrictions.

[0203] FIG. 7 is a schematic structural diagram of a payment card trust evaluation apparatus, according to an embodiment of the present application. Referring to FIG. 7, in a software implementation, a payment card trust evaluation apparatus may include:

[0204] a receiving unit 710 configured to receive a trust evaluation parameter acquisition request for a payment card sent by a payment server, where the trust evaluation parameter acquisition request is sent by the payment server when receiving a payment success indication fed back by a payment ecosystem; and

[0205] a sending unit 720 configured to send, to the payment server based on the trust evaluation parameter acquisition request, trust evaluation parameters corresponding to the payment card and the payment client account, where the trust evaluation parameters are used by the payment server to bind the payment client account to the payment card and determine payment limit restrictions.

[0206] In an embodiment of the present application, by receiving a trust evaluation parameter acquisition request sent by the payment server when the payment card is valid, the trust evaluation parameters are fed back to the payment server, for the payment server to bind the payment card based on the trust evaluation parameters. Therefore, a new card binding process is simplified, and a payment risk after the new card is bound is reduced.

[0207] Optionally, the trust evaluation parameter acquisition request includes at least one of device data, environment data, and account data of the payment client, and a payment

card identifier.

[0208] Optionally, the payment card trust evaluation apparatus may further include a determining unit 730.

[0209] The determining unit 730 determines a device trust level based on the device data of the payment client;

[0210] determines an environment trust level based on the environment data of the payment client;

[0211] determines an account trust level based on the account data of the payment client; and

[0212] determines the trust evaluation parameters based on the device trust level, the environment trust level, and the account trust level.

[0213] Optionally, the trust evaluation parameters include at least one of the following: a payment card trust level and payment restrictions associated with the payment card trust level.

[0214] Optionally, the determining unit 730 may further adjust, based on payment refusal data, transaction data, and trust evaluation parameters, the trust evaluation parameters corresponding to the payment card and the payment client account after the payment card is bound to the payment client account.

[0215] Optionally, the receiving unit 710 is further configured to: receive a verification request sent by the payment server, the verification request being used to request to perform verification to determine whether to allow a payment request for the payment card under the payment client account.

[0216] The sending unit 720 is further configured to: feed a response to the verification request back to the payment server based on current trust evaluation parameters of the payment card and the payment client account.

[0217] For the payment card trust evaluation apparatus, the method in FIG. 3 may be further performed, and the functions of the risk control system in the embodiments shown in FIG. 3 and FIG. 2 are implemented, and details are not described again in the embodiment of the present application.

[0218] The foregoing descriptions are merely preferred embodiments of the present application and are not intended to limit the protection scope of the present application. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of the present application shall fall within the protection scope of the present application.

[0219] The system, the apparatus, the module or the unit described in the foregoing embodiments can be specifically implemented by a computer chip or an entity or implemented by a product having a certain function. A typical implementation device is a computer. Specifically, the computer can be, for example, a personal computer, a laptop computer, a cellular phone, a camera phone, a smartphone, a personal digital assistant, a media player, a navigation device, an email device, a game console, a tablet computer, a wearable device, or a combination of any of these devices.

[0220] The computer readable medium includes a persistent medium and a non-persistent medium, a removable medium and a non-removable medium, which may implement storage of information by using any method or technology. The information may be a computer readable instruction, a data structure, a module of a program or other data. Examples of computer storage media include but are not limited to a phase change memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), other type of random access memory (RAM), a read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a flash memory or other memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or other optical storage, a cassette magnetic tape, tape and disk storage or other magnetic storage device or any other non-transmission media that may be configured to store information that a computing device can access. Based on the definition in the present specification, the computer-readable medium does not include transitory computer readable media (transitory media), such as a modulated data signal and a carrier.

[0221] It should also be noted that the terms “include”, “comprise” and any other variants mean to cover the non-exclusive inclusion. Thereby, the process, method, article, or device which include a series of elements not only include those elements, but also include other elements which are not clearly listed, or include the inherent elements of the process, method, article and device. Without further limitation, the element defined by a phrase “include one” does not exclude other same elements in the process, method, article or device which include the element.

[0222] The embodiments in the present specification are all described in a progressive manner, for same or similar parts in the embodiments, refer to these embodiments, and descriptions of each embodiment focus on a difference from other embodiments. Especially, a system embodiment is basically similar to a method embodiment, and therefore is described briefly; for related parts, reference may be made to partial descriptions in the method embodiment.

CLAIMS

What is claimed is:

1. A payment card binding method, comprising:

sending, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem, wherein the payment card binding request comprises account data of a payment account associated with the payment client, device data of the payment client, and environment data of the payment client;

when the payment is successful, determining (1) an account trust level based on the account data, (2) a device trust level based on the device data, and (3) an environment trust level based on the environment data;

inputting the determined account trust level, the determined device trust level, and the determined environment trust level into a trained new card trust level (NCTL) model to determine a NCTL; and

determining, based on the NCTL, a payment limit restriction of the payment account;

binding, based on the NCTL and the payment limit restriction, the payment account with the payment card to use the payment card for future payments.

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

recharging a payment amount in the first payment request into the payment account.

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

sending, to the payment ecosystem, a second payment request about the payment card under the payment account; and

performing a trust evaluation on the second payment request to determine whether to allow the second payment request.

4. The method according to claim 3, further comprising: if the second payment request is not allowed, performing offsetting on the payment ecosystem based on the second payment request.

5. The method according to claim 3, wherein the performing a trust evaluation on the second payment request to determine whether to allow the second payment request comprises:

sending a verification request for the second payment request to a risk control system, the verification request comprising a payment card identifier, the payment account, and a payment amount of the second payment request; and

receiving, from the risk control system, a response to the verification request, wherein the response is determined by the risk control system based on the determined account trust level,

the determined device trust level, and the determined environment trust level, and the payment amount of the second payment request.

6. A payment card binding apparatus, comprising:

a payment unit configured to send, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem, wherein the payment card binding request comprises account data of a payment account associated with the payment client, device data of the payment client, and environment data of the payment client;

a determining unit configured to: when the payment is successful, determine (1) an account trust level based on the account data, (2) a device trust level based on the device data, and (3) an environment trust level based on the environment data, wherein the determined account trust level, the determined device trust level, and the determined environment trust level are input into a trained new card trust level (NCTL) model to determine a NCTL; and

a binding unit configured to bind, based on the NCTL and the payment limit restriction, the payment account with the payment card to use the payment card for future payments.

7. A computer-readable storage medium storing one or more programs that, when executed by an electronic device comprising a plurality of application programs, cause the electronic device to perform the following operations:

sending, based on a payment card binding request sent by a payment client, a first payment request to a payment ecosystem, wherein the payment card binding request comprises account data of a payment account associated with the payment client, device data of the payment client, and environment data of the payment client;

when the payment is successful, determining (1) an account trust level based on the account data, (2) a device trust level based on the device data, and (3) an environment trust level based on the environment data;

inputting the determined account trust level, the determined device trust level, and the determined environment trust level into a trained new card trust level (NCTL) model to determine a NCTL; and

determining, based on the NCTL, a payment limit restriction of the payment account;

binding, based on the NCTL and the payment limit restriction, the payment account with the payment card to use the payment card for future payments.