支付卡的绑定方法、信任评估方法、装置和电子设备

技术领域

[01]本申请涉及计算机软件技术领域，尤其涉及一种支付卡的绑定方法、信任评估方法、装置和电子设备。

背景技术

[02]用户在使用数字钱包进行支付时，往往需要绑定一张以上的支付卡。

[03]当用户将新的支付卡绑定到数字钱包时，目前大部分使用的验证方法是三域安全（3-D Secure）和宏观支付(Micro Charge)。

[04]3-D Secure: 基于三域模型的认证过程，该三域包括收单机构域（Acquirer Domain）、发行机构域（Issuer Domain）和互操作性域（Interoperability Domain）。

[05]Micro Charge: 数字钱包向用户的信用卡进行随机小额支付，请检查用户是否知道用于认证的金额。

[06]但是，这两种验证方法的验证方式都较为繁琐，用户的掉单率（放弃卡绑定和支付的概率）较高。据统计，两种方案的掉单率都在30-40%以上。

发明内容

[07]本申请实施例的目的是提供一种支付卡的绑定方法、信任评估方法、装置和电子设备，以实现对绑定新卡流程的简化，并减小支付风险。

[08]为解决上述技术问题，本申请实施例是这样实现的:

[09]第一方面，提出了一种支付卡绑定的方法，该方法包括:

[10]基于支付客户端发送的支付卡绑定请求，向支付生态系统发送第一支付请求;

[11]当支付成功时，基于该支付客户端的设备数据、环境数据、账户数据中的至少一种，确定支付卡和支付客户端账户对应的信任评估参数;

[12]基于该信任评估参数对该支付客户端账户与该支付卡进行绑定设置，该信任评估参数用于确定支付额度限制。

[13]第二方面，提出了一种支付卡信任评估方法，该方法包括：

[14]接收支付服务端发送的支付卡的信任评估参数获取请求，其中，该信任评估参数获取请求是该支付服务端在收到支付生态系统反馈的支付成功的指示时发送的；

[15]基于该信任评估参数获取请求，向该支付服务端发送该支付卡和该支付客户端账户对应的信任评估参数，该信任评估参数用于支付服务端对支付客户端的账户与支付卡进行绑定设置，并确定支付额度限制。

[16]第三方面，提出了一种支付卡绑定装置，该装置包括：

[17]支付单元，基于支付客户端发送的支付卡绑定请求，向支付生态系统发送第一支付请求；

[18]确定单元，当支付成功时，基于该支付客户端的设备数据、环境数据、账户数据中的至少一种，确定支付卡和支付客户端账户对应的信任评估参数；

[19]绑定单元，基于该信任评估参数对该支付客户端账户与该支付卡进行绑定设置，该信任评估参数用于确定支付额度限制。

[20]第四方面，提出了一种支付卡信任评估装置，该装置包括：

[21]接收单元，接收支付服务端发送的支付卡的信任评估参数获取请求，其中，该信任评估参数获取请求是该支付服务端在收到支付生态系统反馈的支付成功的指示时发送的；

[22]发送单元，基于该信任评估参数获取请求，向该支付服务端发送该支付卡和该支付客户端账户对应的信任评估参数，该信任评估参数用于支付服务端对支付客户端的账户与支付卡进行绑定设置，并确定支付额度限制。

[23]第五方面，提出了一种电子设备，该电子设备包括：

[24]处理器；以及

[25]被安排成存储计算机可执行指令的存储器，该可执行指令在被执行时使该处理器执行以下操作：

[26]基于支付客户端发送的支付卡绑定请求，向支付生态系统发送第一支付请求；

[27]当支付成功时，基于该支付客户端的设备数据、环境数据、账户数据中的至少一种，确定支付卡和支付客户端账户对应的信任评估参数；

[28]基于该信任评估参数对该支付客户端账户与该支付卡进行绑定设置，该信任评估参数用于确定支付额度限制。

[29]第六方面，提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序当被包括多个应用程序的电子设备执行时，使得该电子设备执行以下操作：

[30]基于支付客户端发送的支付卡绑定请求，向支付生态系统发送第一支付请求；

[31]当支付成功时，基于该支付客户端的设备数据、环境数据、账户数据中的至少一种，确定支付卡和支付客户端账户对应的信任评估参数；

[32]基于该信任评估参数对该支付客户端账户与该支付卡进行绑定设置，该信任评估参数用于确定支付额度限制。

[33]第七方面，提出了一种电子设备，该电子设备包括：

[34]处理器；以及

[35]被安排成存储计算机可执行指令的存储器，该可执行指令在被执行时使该处理器执行以下操作：

[36]接收支付服务端发送的支付卡的信任评估参数获取请求，其中，该信任评估参数获取请求是该支付服务端在收到支付生态系统反馈的支付成功的指示时发送的；

[37]基于该信任评估参数获取请求，向该支付服务端发送该支付卡和该支付客户端账户对应的信任评估参数，该信任评估参数用于支付服务端对支付客户端的账户与支付卡进行绑定设置，并确定支付额度限制。

[38]第八方面，提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序当被包括多个应用程序的电子设备执行时，使得该电子设备执行以下操作：

[39]接收支付服务端发送的支付卡的信任评估参数获取请求，其中，该信任评估参数获取请求是该支付服务端在收到支付生态系统反馈的支付成功的指示时发送的；

[40]基于该信任评估参数获取请求，向该支付服务端发送该支付卡和该支付客户端账户对应的信任评估参数，该信任评估参数用于支付服务端对支付客户端的账户与支付卡进行绑定设置，并确定支付额度限制。

[41]由以上本申请实施例提供的技术方案可见，本申请实施例方案至少具备如下一种技术效果：

[42]第一方面，通过对支付客户端待绑定的支付卡发起支付以确定支付卡的有效性，并基于支付客户端账户数据、支付客户端所在设备数据、支付客户端所在环境数据中的至少一种确定支付卡的信任评估参数，从而能够简化绑定流程，同时减少新卡绑定后的支付风险。

[43]第二方面，通过在接收到支付服务端于支付卡有效时发送的信任评估参数获取请求，向支付服务端反馈信任评估参数，以使得支付服务端能够基于信任评估参数绑定支付卡，从而能够简化新卡绑定流程，同时减小新卡绑定后的支付风险。

附图说明

[44]为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[45]图 1 是本申请的一个实施例支付卡绑定的方法流程图。

[46]图 2 是本申请的一个实施例支付卡绑定及支付卡信任评估的交互流程图。

[47]图 3 是本申请的一个实施例支付卡信任评估的方法流程图。

[48]图 4 是本申请的一个实施例电子设备的结构示意图。

[49]图 5 是本申请的一个实施例支付卡绑定装置的结构示意图。

[50]图 6 是本申请的一个实施例电子设备的结构示意图。

[51]图 7 是本申请的一个实施例支付卡信任评估装置的结构示意图。

具体实施方式

[52]本申请实施例提供一种支付卡的绑定方法、信任评估方法、装置和电子设备。

[53]为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实

施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

[54]图 1 是本申请的一个实施例支付卡绑定的方法流程图。图 1 的方法可应用于支付服务端，例如电子钱包服务器、支付宝系统服务器，等等。图 1 的方法可包括:

[55]S110，基于支付客户端发送的支付卡绑定请求，向支付生态系统发送第一支付请求。

[56]应理解，在本申请实施例中，支付客户端，可以是电子钱包客户端等。在支付客户端账户中，用户可绑定新的支付卡，例如信用卡、借记卡、Visa 卡等等。此时，用户可通过向支付服务端发送支付卡绑定请求以进行支付卡的绑定流程。

[57]应理解，在本申请实施例中，支付生态系统指支付服务提供方，可包括收单方、卡组织和发卡方（发卡银行）等。应理解，收单方可向商户提供支付和清算服务，并把交易转发给连接卡组织；卡组织可将交易转给发卡方，并负责和收单方、发卡方之间的清算；发卡方则负责向消费者提供卡产品，例如在银行办的银行卡，等等。当然，应理解，对于支付生态系统之间的交易流程，本申请实施例对此不作限制，也不排除支付生态系统还存在其它可能的实现方式。

[58]当支付服务端收到支付客服端发送的支付卡绑定请求后，可向支付生态系统发送第一支付请求，以验证支付卡的有效性。

[59]应理解，在发送第一支付请求时，支付服务端可发起一笔小额支付请求，以验证支付卡的有效性。支付服务端可通过扣款交易报文，向支付生态系统发起支付请求（扣款请求）。如果支付生态系统响应于该支付请求，反馈支付成功的结果，则表示支付卡有效；反之，如果支付生态系统反馈支付失败的结果，则表示支付卡无效，此时，不再执行后续的步骤。

[60]应理解，支付请求中的金额，可以是固定的，也可以是随机的。例如，随机发送一笔 0.13 元的扣款，等等。

[61]S120，当支付成功时，基于该支付客户端的设备数据、环境数据、账户数据中的至少一种，确定支付卡和支付客户端账户对应的信任评估参数。

[62]应理解，支付客户端的设备数据，例如，可包括: 设备 ID、设备 MAC 地址，等等。

[63]基于支付客户端的设备数据，可确定设备信任级别。

[64]例如，设备是支付客户端账户的常用设备，设备信任级别较高，对应的信任评估参数也会较高；如果设备是支付客户端账户第一次使用的设备，则设备信任级别较低，对应的信任评估参数也会较低。又例如，该设备曾经有欺诈历史，则其设备信任级别较低，对应的信任评估参数也会较低，等等。

[65]支付客户端的环境数据，例如，可包括：支付客户端所在的终端设备连接的 WIFI 的名字，WIFI 的 MAC 地址，设备所在的地理位置（经纬度信息），IP 地址段等。

[66]基于支付客户端的环境数据，也可确定环境信任级别。

[67]类似地，如果环境数据表明用户不在常驻地点，例如国外，则其环境信任级别就较低，对应的信任评估参数也会较低。

[68]支付客户端账户数据，例如，可包括：支付客户端账户 ID、注册时间、客户的姓名、性别、地址、年龄、资金渠道，客户资料修改的历史记录，等等。

[69]基于支付客户端的账户数据，也可确定账户信任级别。

[70]例如，支付客户端账户对应的年龄在 30 岁-40 岁之间，则账户信任级别较高；支付客户端账户对应的年龄在 8 岁-12 岁之间，则账户信任级别较低。又例如，支付客户端账户有过欺诈历史，则账户信任级别较低，等等。

[71]基于设备数据、环境数据、账户数据中的一种或多种，可确定支付卡和支付客户端账户对应的信任评估参数。

[72]S130，基于该信任评估参数对该支付客户端账户与该支付卡进行绑定设置。

[73]其中，该信任评估参数用于确定支付额度限制。

[74]在确定信任评估参数后，即可基于信任评估参数，对该支付客户端账户与该支付卡进行绑定设置。

[75]可选地，该信任评估参数包括以下至少一种：支付卡的信任等级、与支付卡的信任等级关联的支付限制。应理解，在绑定新卡的流程中，风险控制系统可将新卡信任等级（New Card Trust Level，NCTL）及 NCTL 对应的支付限制中的至少一种反馈给支付服务端。

[76]相应地，步骤 S130 可实现为：

[77]在绑定该支付客户端账户与该支付卡时，基于该信任评估参数，设定该支付卡在该

支付客户端账户中的信任等级、支付限制中的至少一个参数。

[78]例如，假设风险控制系统对 NCTL 的级别分为 0、1、2、3、4 五级，NCTL 级别越高，信任度越高，风险越小。不妨还假设 NCTL 各级别对应的支付限制分别为 0 元，100 元，500 元，1000 元，2000 元。当风险控制系统基于支付客户端的设备数据、该支付客户端的环境数据、支付卡标识、支付客户端账户数据等确定 NCTL 为 1 级时，可将 1 级反馈给支付服务端，或将支付限制 100 元反馈给支付服务端，或者将 1 级和 100 元这两个信息一起反馈给支付服务端。当然，应理解，在这个示例中，如果确定 NCTL 为 0 级，说明支付卡可信度极低，绑定支付卡的支付客户端账户存在较高的风险。

[79]本申请实施例中，通过对支付客户端待绑定的支付卡发起支付以确定支付卡的有效性，并基于支付客户端账户数据、支付客户端所在设备数据、支付客户端所在环境数据中的至少一种确定支付卡的信任评估参数，从而能够简化绑定流程，同时减少新卡绑定后的支付风险。

[80]可选地，作为一个实施例，支付服务端中可包括风险控制模块，用于基于该支付客户端的设备数据、环境数据、账户数据中的至少一种，确定支付卡和支付客户端账户对应的信任评估参数。

[81]可选地，作为另一个实施例，支付服务端中不具备风险控制模块。此时，步骤 S120 可实现为:

[82]向风险控制系统发送关于支付卡和支付客户端账户的信任评估参数获取请求，该信任评估参数获取请求携带有该支付客户端的设备数据、环境数据、账户数据中的至少一种，以及该支付卡标识;

[83]接收该风险控制系统基于该信任评估参数获取请求反馈的信任评估参数。

[84]可选地，在步骤 S130 之后，该方法还可包括:

[85]将该第一支付请求中的支付金额充值到该支付客户端账户中。

[86]可选地，在步骤 S130 之后，该方法还可包括:

[87]向该支付生态系统发送该支付客户端账户下关于该支付卡的第二支付请求;

[88]对该第二支付请求进行信任评估，以确定是否允许该第二支付请求。

[89]应理解，当支付服务端接收到支付客户端账户发送的关于该支付卡的支付请求时，

可将该支付请求发送给风险控制系统，以对该支付请求进行风险校验。风险控制系统可基于该支付卡的拒付数据、交易数据及支付卡信任级别等数据，以及支付请求中携带的支付额度，确定是否允许该支付。通过风险控制系统对支付请求的风险校验，可进一步减少支付卡绑定后的支付风险。

[90]进一步地，该方法还包括：如果不允许该第二支付请求，则基于该第二支付请求向该支付生态系统进行冲账处理。

[91]当然，应理解，在对该第二支付请求进行信任评估，以确定是否允许该第二支付请求的步骤中，当支付服务端不具备风险控制模块时，该步骤可实现为：

[92]向风险控制系统发送第二支付请求的校验请求，该校验请求中携带该支付卡标识、该支付客户端账户及该第二支付请求的支付金额；

[93]接收该风险控制系统对该校验请求的响应，其中，该响应由该风险控制系统基于该支付卡和该支付客户端账户对应的信任评估参数，以及该第二支付请求的支付金额确定。

[94]可选地，该响应中还可携带该风险控制系统调整后的信任评估参数；该方法还包括：

[95]基于该调整后的信任评估参数对该支付客户端账户与该支付卡进行绑定参数的重设置。

[96]相应地，如果支付服务端具备风险控制模块，则在步骤 S130 之后，该方法还可包括：

[97]基于该支付卡绑定到该支付客户端账户后的拒付数据、交易数据和信任评估参数，调整该支付卡和该支付客户端账户对应的信任评估参数。

[98]通过基于拒付数据、交易数据及当前信任评估参数来得到调整后的信任评估参数，可以使得绑定的支付卡随着交易次数的增多调整支付限制，从而使得支付限制与支付客户端账户、支付卡、设备、环境等多方面的因素相匹配。

[99]下面，将结合具体的实施例，对本申请实施例的方法作进一步的描述。

[100] 图 2 是本申请的一个实施例支付卡绑定和支付卡信任评估的交互流程图。在图 2 所示的实施例中，可包括钱包客户端、钱包服务端、支付生态系统和风险控制系统四方的信息交互。其中，

[101] 钱包客户端，即图 1 所示实施例的支付客户端，可用于发起绑定新卡请求。

[102] 钱包服务器，即图 1 所示实施例的支付服务端，可响应钱包客户端的绑定新卡请求，进行新卡绑定的相关操作。

[103] 支付生态系统，即图 1 所示实施例的支付生态系统，是支付服务的提供方。在图 2 所示实施例中，支付生态系统可包括收单方、卡组织和发卡方，其中，收单方可向商户提供支付和清算服务，并把交易转发给连接卡组织；卡组织可将交易转给发卡方，并负责和收单方、发卡方之间的清算；发卡方则负责向消费者提供卡产品，例如在银行办的银行卡，等等。

[104] 风险控制系统，即图 1 所示实施例的风险控制系统，用于实时计算和更新 NCTL 的钱包帐户、设备和环境的信任等级，以更新 NCTL 和 NCTL 关联支出限制，并作为钱包服务器的响应。风险控制系统可提供一个 API 接口，钱包服务器可通过该 API 接口获取新卡和钱包客户端账户对应的 NCTL 和/或 NCTL 对应的支付限制。

[105] 下面，将详细介绍方案流程。

[106] 步骤 1：钱包客户端向钱包服务器发送新卡绑定请求。

[107] 应理解，钱包客户端在发送新卡绑定请求时，可将钱包客户端的账户标识和待绑定的支付卡相关参数发送给钱包服务器。

[108] 支付卡相关参数，例如，支付卡标识、支付卡密码。当然，支付卡相关参数还可包括支付卡的校验码、支付卡在发卡银行绑定的手机号码、支付卡的用户的身份标识等信息中的至少一种。

[109] 当然，应理解，钱包客户端还可将钱包客户端的其它账户数据发送给钱包服务器。

[110] 钱包客户端还可将设备数据发送给钱包客户端。设备数据，例如，钱包客户端所在的终端设备的设备标识、MAC 地址等等。

[111] 钱包客户端还可将环境数据发送给钱包客户端。环境数据，例如，钱包客户端所在的终端设备连接的 WIFI 的名字，WIFI 的 MAC 地址，设备所在的地理位置（经纬度信息），IP 地址段等。设备所在的地理位置，例如，可以通过终端设备的定位功能（Location Based Service，LBS）得到。

[112] 步骤 2：钱包服务端向支付生态系统发送支付请求。

[113] 钱包服务端基于钱包客户端的新卡绑定请求，可向支付生态系统发送支付请求，

以校验新卡的有效性。

[114] 一个具体的例子，钱包服务端可通过一个扣款交易报文，向支付生态系统发送扣款请求，以校验新卡的有效性。例如，支付服务端可通过发起一笔很小的随机支付金额，例如 0.13 元，等等。。

[115] 支付生态系统根据扣款交易报文，可返回扣款成功或扣款失败的响应。其处理的具体方式可参考现有技术，本申请实施例在此不再赘述。

[116] 步骤 3：钱包服务端向风险控制系统发送信任评估参数获取请求。

[117] 在图 2 所示实施例中，钱包服务端可通过调用 NCTL Risk Service API，向风险控制系统发送信任评估参数获取请求，以获取新卡和钱包客户端账户对应的信任评估参数。

[118] 如图 2 所示，作为 NCTL Risk Service API 的输入，可包括新卡标识、钱包客户端账户数据、设备数据和环境数据。

[119] 步骤 4：风险控制系统计算信任评估参数。

[120] 风险控制系统基于钱包客户端账户数据，可计算得到账户信任级别（Account Trust Level，ATL）；

[121] 风险控制系统基于设备数据，可计算得到设备信任级别（Device Trust Level，DTL）；

[122] 风险控制系统基于环境数据，可计算得到环境信任级别（Environment Trust Level，ETL）。

[123] 在计算 ATL、DTL 和 ETL 时，可基于对应的信任等级计算模型得到。

[124] 基于 ATL、DTL 和 ETL，风险控制系统可得到对应的 NCTL。计算 NCTL 的方式，也可基于 NCTL 模型得到。

[125] 上述模型的训练方式，可基于对应的训练数据得到，本申请实施例在此不作限制。

[126] 当然，应理解，确定 NCTL 的参数，可以只包括 ATL、DTL 和 ETL 中的一种或多种，还可以包括 ATL、DTL 和 ETL 以外的其它参数，本申请实施例对此不作限制。

[127] 此外，基于 NCTL，风险控制系统还可确定 NCTL 对应的支付限额。

[128] 步骤 5：风险控制系统反馈信任评估参数。

[129] 如图 2 所示，风险控制系统可将 NCTL 和 NCTL 对应的支付限制反馈给钱包服务器。当然，应理解，风险控制系统也可只将 NCTL 和支付限制的其中一个反馈给钱包服务器。

[130] 步骤 6：钱包服务器绑定支付卡和钱包客户端账户。

[131] 钱包服务器基于风险控制系统反馈的信任评估参数，可对支付卡和钱包客户端账户进行绑定参数，并设定对应的绑定参数，例如，NCTL、支付限制，等等。

[132] 至此，完成了支付卡的绑定流程。

[133] 此外，应理解，在后续的支付流程中，支付服务端也可参照图 2 所示的方案向支付生态系统发起支付请求，然后将支付请求发送给风险控制系统进行校验。风险控制系统可基于支付卡和钱包客户端账户当前的 NCTL 和支付限制，确定是否允许该支付请求。如果不允许，则向支付生态系统发起冲账处理。

[134] 当然，应理解，风险控制系统还可基于支付卡绑定到钱包客户端账户后产生的拒付记录、交易记录及当前的 NCTL，调整支付卡和钱包客户端账户对应的 NCTL。

[135] 此外，应理解，上述实施例中的支付服务端与风险控制系统，也可以合并为一个系统。

[136] 图 3 是一种支付卡的信任评估方法流程图。图 3 的方法由风险控制系统执行。该方法可包括:

[137] S310，接收支付服务端发送的支付卡的信任评估参数获取请求。

[138] 其中，该信任评估参数获取请求是该支付服务端在收到支付生态系统反馈的支付成功的指示时发送的。

[139] S320，基于该信任评估参数获取请求，向该支付服务端发送该支付卡和该支付客户端账户对应的信任评估参数。

[140] 其中，该信任评估参数用于支付服务端对支付客户端的账户与支付卡进行绑定设置，并确定支付额度限制。

[141] 本申请实施例中，通过在接收到支付服务端于支付卡有效时发送的信任评估参数获取请求，向支付服务端反馈信任评估参数，以使得支付服务端能够基于信任评估参

数绑定支付卡，从而能够简化新卡绑定流程，同时减小新卡绑定后的支付风险。

[142] 可选地，该信任评估参数获取请求携带有：该信任评估参数获取请求携带有该支付客户端的设备数据、环境数据、账户数据中的至少一种，以及该支付卡标识。

[143] 可选地，步骤 S320 具体可实现为：

[144] 基于该支付客户端的设备数据确定设备信任级别；

[145] 基于该支付客户端的环境数据确定环境信任级别；

[146] 基于该支付客户端的账户数据确定账户信任级别；

[147] 基于设备信任级别、环境信任级别和账户信任级别，确定该信任评估参数。

[148] 当然，应理解，也可基于设备信任级别、环境信任级别、账户信任级别中的一个或两个，确定该信任评估参数。

[149] 可选地，该信任评估参数包括以下至少一种：支付卡的信任等级、与支付卡的信任等级关联的支付限制。

[150] 可选地，该方法还可包括：

[151] 基于该支付卡绑定到该支付客户端账户后的拒付数据、交易数据和信任评估该参数，调整该支付卡和该支付客户端账户对应的信任评估该参数

[152] 可选地，该方法还可包括：

[153] 接收支付服务端发送的校验请求，该校验请求用于请求校验是否允许该支付客户端账户下关于该支付卡的支付请求；

[154] 基于该支付卡和该支付客户端账户当前的信任评估该参数，向该支付服务端反馈该校验请求的响应。

[155] 图 3 所示实施例的具体实现可参考图 1、图 2 所示实施例中风险控制系统执行的方法，本申请实施例在此不再赘述。

[156] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[157] 图 4 是本申请的一个实施例电子设备的结构示意图。请参考图 4，在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器（non-volatile memory），例如至少 1 个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

[158] 处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是 ISA(Industry Standard Architecture，工业标准体系结构）总线、PCI(Peripheral Component Interconnect，外设部件互连标准)总线或 EISA(Extended Industry Standard Architecture，扩展工业标准结构）总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 4 中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

[159] 存储器，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器，并向处理器提供指令和数据。

[160] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成支付卡绑定装置。处理器，执行存储器所存放的程序，并具体用于执行以下操作:

[161] 基于支付客户端发送的支付卡绑定请求，向支付生态系统发送第一支付请求;

[162] 当支付成功时，基于该支付客户端的设备数据、环境数据、账户数据中的至少一种，确定支付卡和支付客户端账户对应的信任评估参数;

[163] 基于该信任评估参数对该支付客户端账户与该支付卡进行绑定设置，该信任评估参数用于确定支付额度限制。

[164] 上述如本申请图 1 所示实施例揭示的支付卡绑定装置执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器（Central Processing Unit，CPU）、网络处理器（Network Processor，NP）等; 还可以是数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field－Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常

规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

[165] 该电子设备还可执行图 1 的方法，并实现支付服务端或钱包服务端在图 1、图 2 所示实施例的功能，本申请实施例在此不再赘述。

[166] 当然，除了软件实现方式之外，本申请的电子设备并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[167] 本申请实施例还提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序包括指令，该指令当被包括多个应用程序的便携式电子设备执行时，能够使该便携式电子设备执行图 1 所示实施例的方法，并具体用于执行以下操作:

[168] 基于支付客户端发送的支付卡绑定请求，向支付生态系统发送第一支付请求;

[169] 当支付成功时，基于该支付客户端的设备数据、环境数据、账户数据中的至少一种，确定支付卡和支付客户端账户对应的信任评估参数;

[170] 基于该信任评估参数对该支付客户端账户与该支付卡进行绑定设置，该信任评估参数用于确定支付额度限制。

[171] 图 5 是本申请的一个实施例支付卡绑定装置的结构示意图。请参考图 5，在一种软件实施方式中，支付卡绑定装置 500 可包括:

[172] 支付单元 510，基于支付客户端发送的支付卡绑定请求，向支付生态系统发送第一支付请求;

[173] 确定单元 520，当支付成功时，基于该支付客户端的设备数据、环境数据、账户数据中的至少一种，确定支付卡和支付客户端账户对应的信任评估参数;

[174] 绑定单元 530，基于该信任评估参数对该支付客户端账户与该支付卡进行绑定设置，该信任评估参数用于确定支付额度限制。

[175] 本申请实施例中，通过对支付客户端待绑定的支付卡发起支付以确定支付卡的

有效性，并基于支付客户端账户数据、支付客户端所在设备数据、支付客户端所在环境数据中的至少一种确定支付卡的信任评估参数，从而能够简化绑定流程，同时减少新卡绑定后的支付风险。

[176] 可选地，确定单元 520 具体用于：

[177] 向风险控制系统发送关于支付卡和支付客户端账户的信任评估参数获取请求，该信任评估参数获取请求携带有该支付客户端的设备数据、环境数据、账户数据中的至少一种，以及该支付卡标识；

[178] 接收该风险控制系统基于该信任评估参数获取请求反馈的信任评估参数。

[179] 可选地，该信任评估参数包括以下至少一种：支付卡的信任等级、与支付卡的信任等级关联的支付限制。

[180] 可选地，绑定单元 530 具体用于：在绑定该支付客户端账户与该支付卡时，基于该信任评估参数，设定该支付卡在该支付客户端账户中的信任等级、支付限制中的至少一个参数。

[181] 可选地，支付卡绑定装置 500 还包括充值单元 540，将该第一支付请求中的支付金额充值到该支付客户端账户中。

[182] 可选地，支付单元 510 还向该支付生态系统发送该支付客户端账户下关于该支付卡的第二支付请求；

[183] 确定单元 520 还对该第二支付请求进行信任评估，以确定是否允许该第二支付请求。

[184] 可选地，支付卡绑定装置 500 还包括冲账单元 550，如果不允许该第二支付请求，则基于该第二支付请求向该支付生态系统进行冲账处理。

[185] 可选地，确定单元 520 还用于：

[186] 向风险控制系统发送第二支付请求的校验请求，该校验请求中携带该支付卡标识、该支付客户端账户及该第二支付请求的支付金额；

[187] 接收该风险控制系统对该校验请求的响应，其中，该响应由该风险控制系统基于该支付卡和该支付客户端账户对应的信任评估参数，以及该第二支付请求的支付金额确定。

[188] 可选地，该响应中还携带该风险控制系统调整后的信任评估参数；绑定单元 530 还用于基于该调整后的信任评估参数对该支付客户端账户与该支付卡进行绑定参数的重设置。

[189] 可选地，该支付生态系统包括收单方子系统、卡方案子系统和发卡方子系统。

[190] 该支付卡绑定装置还可执行图 1 的方法，并实现支付服务端或钱包服务端在图 1、图 2 所示实施例的功能，本申请实施例在此不再赘述。

[191] 图 6 是本申请的一个实施例电子设备的结构示意图。请参考图 6，在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器（non-volatile memory），例如至少 1 个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

[192] 处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是 ISA(Industry Standard Architecture，工业标准体系结构）总线、PCI(Peripheral Component Interconnect，外设部件互连标准)总线或 EISA(Extended Industry Standard Architecture，扩展工业标准结构）总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 6 中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

[193] 存储器，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器，并向处理器提供指令和数据。

[194] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成支付卡信任评估装置。处理器，执行存储器所存放的程序，并具体用于执行以下操作：

[195] 接收支付服务端发送的支付卡的信任评估参数获取请求，其中，该信任评估参数获取请求是该支付服务端在收到支付生态系统反馈的支付成功的指示时发送的；

[196] 基于该信任评估参数获取请求，向该支付服务端发送该支付卡和该支付客户端账户对应的信任评估参数，该信任评估参数用于支付服务端对支付客户端的账户与支付卡进行绑定设置，并确定支付额度限制。

[197] 上述如本申请图 3 所示实施例揭示的支付卡信任评估装置或风险控制系统执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具

有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器（Central Processing Unit，CPU）、网络处理器（Network Processor，NP）等；还可以是数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field－Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

[198] 该电子设备还可执行图 3 的方法，并实现风险控制系统在图 3、图 2 所示实施例的功能，本申请实施例在此不再赘述。

[199] 当然，除了软件实现方式之外，本申请的电子设备并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[200] 本申请实施例还提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序包括指令，该指令当被包括多个应用程序的便携式电子设备执行时，能够使该便携式电子设备执行图 3 所示实施例的方法，并具体用于执行以下操作：

[201] 接收支付服务端发送的支付卡的信任评估参数获取请求，其中，该信任评估参数获取请求是该支付服务端在收到支付生态系统反馈的支付成功的指示时发送的；

[202] 基于该信任评估参数获取请求，向该支付服务端发送该支付卡和该支付客户端账户对应的信任评估参数，该信任评估参数用于支付服务端对支付客户端的账户与支付卡进行绑定设置，并确定支付额度限制。

[203] 图 7 是本申请的一个实施例支付卡信任评估装置的结构示意图。请参考图 7，在一种软件实施方式中，支付卡信任评估装置可包括：

[204] 接收单元 710，接收支付服务端发送的支付卡的信任评估参数获取请求，其中，

该信任评估参数获取请求是该支付服务端在收到支付生态系统反馈的支付成功的指示时发送的；

[205] 发送单元720，基于该信任评估参数获取请求，向该支付服务端发送该支付卡和该支付客户端账户对应的信任评估参数，该信任评估参数用于支付服务端对支付客户端的账户与支付卡进行绑定设置，并确定支付额度限制。

[206] 本申请实施例中，通过在接收到支付服务端于支付卡有效时发送的信任评估参数获取请求，向支付服务端反馈信任评估参数，以使得支付服务端能够基于信任评估参数绑定支付卡，从而能够简化新卡绑定流程，同时减小新卡绑定后的支付风险。

[207] 可选地，该信任评估参数获取请求携带有该支付客户端的设备数据、环境数据、账户数据中的至少一种，以及该支付卡标识。

[208] 可选地，支付卡信任评估装置还可包括确定单元730，其中，

[209] 确定单元730，基于该支付客户端的设备数据确定设备信任级别；

[210] 基于该支付客户端的环境数据确定环境信任级别；

[211] 基于该支付客户端的账户数据确定账户信任级别；

[212] 基于设备信任级别、环境信任级别和账户信任级别，确定该信任评估参数。

[213] 可选地，该信任评估参数包括以下至少一种：支付卡的信任等级、与支付卡的信任等级关联的支付限制。

[214] 可选地，确定单元730，还可基于该支付卡绑定到该支付客户端账户后的拒付数据、交易数据和信任评估该参数，调整该支付卡和该支付客户端账户对应的信任评估该参数。

[215] 可选地，接收单元710还用于：接收支付服务端发送的校验请求，该校验请求用于请求校验是否允许该支付客户端账户下关于该支付卡的支付请求；

[216] 发送单元720还用于：基于该支付卡和该支付客户端账户当前的信任评估该参数，向该支付服务端反馈该校验请求的响应。

[217] 该支付卡信任评估装置还可执行图3的方法，并实现风险控制系统在图3、图2所示实施例的功能，本申请实施例在此不再赘述。

[218] 总之，以上所述仅为本申请的较佳实施例而已，并非用于限定本申请的保护范

围。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

[219] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[220] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[221] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[222] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。