

一种离线支付的授权、离线支付、收款方法及装置

5 本申请要求于2021年09月27日提交中国国家知识产权局、申请号为202111147591.1、
申请名称为“一种离线支付的授权、离线支付、收款方法及装置”的中国专利申请的优
先权，其全部内容通过引用结合在本申请中。

技术领域

10 本说明书涉及电子支付技术领域，尤其涉及一种离线支付的授权、离线支付、针
对离线设备的收款方法及装置。

背景技术

无网状态下使用离线钱包支付（离线支付）是对有网支付的一个重要补充。无网
状态一般发生在特定场景下，例如：飞机上、地下室以及山区等。

15 目前使用离线钱包支付的方案，都需要在终端设备处于联网的状态下激活离线钱
包（即开立离线账户）并且“充值”一定数额的钱到离线钱包上，进而，在终端设备
处于无网状态下，供用户使用离线钱包支付服务。

然而，提前激活离线钱包并充值对离线钱包支付的实际场景应用存在一定程度上
的使用限制。

20 **发明内容**

本说明书一个或多个实施例提供了一种离线支付的授权、离线支付、针对离线设
备的收款方法及装置，以实现免提前充值的离线支付功能的授权。

根据第一方面，提供一种离线支付的授权方法，应用于服务器，所述方法包括：

25 在检测到目标电子钱包账户的当前状态满足预设证书下发条件时，获得所述目标
电子钱包账户的钱包账户信息、当前账户余额及当前信用信息；

基于所述当前账户余额以及所述当前信用信息，确定对应的可离线支付额度；

利用服务器私钥，对汇总信息进行签名，得到电子钱包签名，所述汇总信息包括，
所述钱包账户信息、所述可离线支付额度、签发时间以及有效时长；

基于所述汇总信息以及所述电子钱包签名，生成用户证书；

30 将所述用户证书下发至所述目标电子钱包账户所在终端设备，以使得所述目标电
子钱包账户对应的离线账户可基于所述用户证书在所述可离线支付额度之内进行离线
支付。

在一种可实施方式中，所述预设证书下发条件包括如下条件中的至少一个：所述
目标电子钱包账户的已获得用户证书过期，且所述终端设备处于联网状态；

- 在所述已获得用户证书到期之前的第一时段，且所述终端设备处于联网状态；
- 在所述已获得用户证书到期之前的第二时段，且所述终端设备的流量使用状态满足预设空闲条件；
- 所述目标电子钱包账户的当前账户余额和/或所述当前信用信息变更达到一定条件；
- 5 所述目标电子钱包账户未获得过用户证书，且所述终端设备的流量使用状态满足预设空闲条件。
- 在一种可实施方式中，所述钱包账户信息为：所述目标电子钱包账户对应的钱包账户 ID 和钱包账户名信息的哈希值。
- 10 在一种可实施方式中，所述当前信用信息包括如下信息中的至少一种：当前的信用值以及当前的可借贷额度。
- 在一种可实施方式中，所述终端设备设置有可信执行环境 TEE；
- 所述将所述用户证书下发至所述目标电子钱包账户所在终端设备，包括：
- 将所述用户证书下发至所述终端设备的 TEE 中，以使所述终端设备在所述 TEE
- 15 中存储所述用户证书。
- 在一种可实施方式中，所述基于所述当前账户余额以及所述当前信用信息，确定对应的可离线支付额度，包括：
- 基于所述当前账户余额、所述当前信用信息及其各自对应的权重，确定所述目标电子钱包账户的账户打分的当前分值；
- 20 基于所述当前分值，确定所述目标电子钱包账户对应的可离线支付额度。
- 在一种可实施方式中，所述基于所述当前分值，确定所述目标电子钱包账户对应的可离线支付额度，包括：
- 基于预设的账户打分与额度等级之间的第一对应关系，确定所述当前分值对应的当前额度等级；
- 25 基于预设的额度等级与额度值的第二对应关系，确定所述当前额度等级对应的额度值，作为所述可离线支付额度。
- 在一种可实施方式中，还包括：
- 获得所述终端设备发送的离线账单，其中，所述离线账单为所述离线账户离线支付生成的账单，至少包括对应的交易金额以及所述钱包账户信息；
- 30 基于所述交易金额以及所述钱包账户信息，从所述目标电子钱包账户中扣除相应的金额；
- 发送额度恢复信息至所述终端设备，以使所述离线账户的当前离线支付的上限，恢复为所述可离线支付额度。

在一种可实施方式中,所述离线账单还包括:相应的商户账户信息以及商户签名,所述商户签名为:利用商户私钥对所述商户账户信息以及所述交易金额签名所得;

所述基于所述交易金额以及所述钱包账户信息,从所述目标电子钱包账户中扣除相应的金额,包括:

- 5 利用所述商户私钥对应的商户公钥,对所述离线账单进行验证;

若验证通过,基于所述交易金额以及所述钱包账户信息,从所述目标电子钱包账户中扣除相应的金额。

- 根据第二方面,提供一种离线支付方法,应用于终端设备,所述终端设备存储有服务器下发的用户证书,所述用户证书至少包括,可离线支付额度、签发时间、有效
10 时长以及电子钱包签名,所述方法包括:

在接收到离线支付指令的情况下,判断所述离线支付指令携带的当前交易金额是否不大于当前离线支付的上限,其中,所述当前离线支付的上限基于所述可离线支付额度以及历史离线交易金额确定;

- 若判断所述当前交易金额不大于所述当前离线支付的上限,将所述用户证书提供
15 至所述离线支付指令对应的收款设备;

获得所述收款设备提供的交易确认信息,其中,所述交易确认信息为所述收款设备基于所述电子钱包签名确定所述用户证书有效的情况下发送的;

基于所述交易确认信息生成离线账单。

- 在一种可实施方式中,所述终端设备包括可信执行环境 TEE,所述用户证书存储
20 在所述 TEE 中,所述方法在所述 TEE 中执行。

在一种可实施方式中,还包括:

基于所述离线支付指令的接收时间、所述用户证书的签发时间及有效时长,判断所述用户证书是否有效;

在确定所述用户证书有效的情况下,将所述用户证书提供至所述收款设备。

- 25 在一种可实施方式中,还包括:

计算所述当前离线支付的上限与所述当前交易金额的差值;

将所述差值确定为新的当前离线支付的上限。

在一种可实施方式中,还包括:

- 在处于联网状态下,将所述离线账单发送至所述服务器,以使所述服务器基于所
30 述离线账单进行清算。

在一种可实施方式中,所述获得所述收款设备提供的交易确认信息,包括:

通过短距离传输方式,获得所述收款设备提供的交易确认信息。

在一种可实施方式中,所述交易确认信息包括:所述商户的商户账户信息、所述

当前交易金额以及商户签名, 所述商户签名为: 利用商户私钥对所述商户账户信息以及所述当前交易金额签名所得;

所述基于所述交易确认信息生成离线账单, 包括:

基于所述商户私钥对应的商户公钥, 对所述交易确认信息进行验证;

- 5 若验证通过, 基于所述商户账户信息、所述当前交易金额以及所述钱包账户信息, 生成离线账单。

根据第三方面, 提供一种针对离线设备的收款方法, 应用于收款设备, 所述方法包括:

- 10 获得离线的终端设备提供的用户证书, 其中, 所述用户证书由服务器下发, 并包括: 所述终端设备对应的电子钱包账户的钱包账户信息、可离线支付金额、所述用户证书的签发时间和有效时长以及电子钱包签名;

利用所述服务器的公钥, 对所述电子钱包签名进行验证;

若验证通过, 基于本次交易的交易时间、所述签发时间及所述有效时长, 判断所述用户证书是否有效;

- 15 在判断所述用户证书有效的情况下, 生成本次交易相应的交易确认信息;

将所述交易确认信息提供至所述终端设备, 以使所述终端设备基于所述交易确认信息生成相应的离线账单。

- 20 在一种可实施方式中, 所述交易确认信息至少包括: 所述商户的商户账户信息、本次交易的交易金额以及商户签名, 所述商户签名为: 利用商户私钥对所述商户账户信息以及所述当前交易金额签名所得。

在一种可实施方式中, 所述将所述交易确认信息提供至所述终端设备, 包括:

通过短距离传输方式, 将所述交易确认信息提供至所述终端设备。

在一种可实施方式中, 还包括:

在判断所述用户证书无效的情况下, 生成交易失败信息;

- 25 将所述交易失败信息提供至所述终端设备。

根据第四方面, 提供一种离线支付的授权装置, 应用于服务器, 所述装置包括:

第一获得模块, 配置为在检测到目标电子钱包账户的当前状态满足预设证书下发条件时, 获得所述目标电子钱包账户的钱包账户信息、当前账户余额及当前信用信息;

- 30 第一确定模块, 配置为基于所述当前账户余额以及所述当前信用信息, 确定对应的可离线支付额度;

第一签名模块, 配置为利用服务器私钥, 对汇总信息进行签名, 得到电子钱包签名, 所述汇总信息包括, 所述钱包账户信息、所述可离线支付额度、签发时间以及有效时长;

第一生成模块,配置为基于所述汇总信息以及所述电子钱包签名,生成用户证书;

第一发送模块,配置为将所述用户证书下发至所述目标电子钱包账户所在终端设备,以使得所述目标电子钱包账户对应的离线账户可基于所述用户证书在所述可离线支付额度之内进行离线支付。

- 5 根据第五方面,提供一种离线支付装置,应用于终端设备,所述终端设备存储有服务器下发的用户证书,所述用户证书至少包括,可离线支付额度、签发时间、有效时长以及电子钱包签名,所述装置包括:

第一判断模块,配置为在接收到离线支付指令的情况下,判断所述离线支付指令携带的当前交易金额是否不大于当前离线支付的上限,其中,所述当前离线支付的上限基于所述可离线支付额度以及历史离线交易金额确定;

- 10 第一提供模块,配置为若判断所述当前交易金额不大于所述当前离线支付的上限,将所述用户证书提供至所述离线支付指令对应的收款设备;

- 15 第二获得模块,配置为获得所述收款设备提供的交易确认信息,其中,所述交易确认信息为所述收款设备基于所述电子钱包签名确定所述用户证书有效的情况下发送的;

第二生成模块,配置为基于所述交易确认信息生成离线账单。

根据第六方面,提供一种针对离线设备的收款装置,应用于收款设备,所述装置包括:

- 20 第三获得模块,配置为获得离线的终端设备提供的用户证书,其中,所述用户证书由服务器下发,并包括:所述终端设备对应的电子钱包账户的钱包账户信息、可离线支付金额、所述用户证书的签发时间和有效时长以及电子钱包签名;

第一验证模块,配置为利用所述服务器的公钥,对所述电子钱包签名进行验证;

第二判断模块,配置为若验证通过,基于本次交易的交易时间、所述签发时间及所述有效时长,判断所述用户证书是否有效;

- 25 第三生成模块,配置为在判断所述用户证书有效的情况下,生成本次交易相应的交易确认信息;

第二提供模块,配置为将所述交易确认信息提供至所述终端设备,以使所述终端设备基于所述交易确认信息生成相应的离线账单。

- 30 根据第七方面,提供一种计算机可读存储介质,其上存储有计算机程序,当所述计算机程序在计算机中执行时,令计算机执行第一方面所述的方法。

根据第八方面,提供一种计算设备,包括存储器和处理器,其中,所述存储器中存储有可执行代码,所述处理器执行所述可执行代码时,实现第一方面所述的方法。

根据第九方面,提供一种计算机可读存储介质,其上存储有计算机程序,当所述计算机程序在计算机中执行时,令计算机执行第二方面所述的方法。

根据第十方面，提供一种计算设备，包括存储器和处理器，其中，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第二方面所述的方法。

根据第十一方面，提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行第三方面所述的方法。

5 根据第十二方面，提供一种计算设备，包括存储器和处理器，其中，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第三方面所述的方法。

根据本说明书实施例提供的方法及装置，在目标电子钱包账户的当前状态满足预设证书下发条件时，利用目标电子钱包账户的钱包账户信息、当前账户余额及当前信用信息，生成目标电子钱包账户对应的包括可离线支付额度的用户证书，并下发至目标电子钱包账户所在终端设备，使得目标电子钱包账户对应的离线账户可基于用户证书在可离线支付额度之内进行离线支付，即通过用户证书实现对离线账户的离线支付授权，使得离线账户无需提前充值即无需提前圈存流动资金，即可实现在可离线支付额度之内的离线支付。并且，在该用户证书为首次针对目标电子钱包账户下发的情况下，还可以实现免开立目标电子钱包账户对应的离线账户（即免激活相应的硬件钱包），实现对该离线账户的免开立及免提前充值的离线支付功能授权。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单的介绍。显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

- 图 1 为本说明书披露的一个实施例的实施框架示意图；
- 图 2 为实施例提供的离线支付的授权方法的一种流程示意图；
- 图 3 为实施例提供的离线支付方法的一种流程示意图；
- 图 4 为实施例提供的针对离线设备的收款方法的一种流程示意图；
- 25 图 5 为实施例提供的离线支付的授权装置的一种示意性框图；
- 图 6 为实施例提供的离线支付装置的一种示意性框图；
- 图 7 为实施例提供的针对离线设备的收款装置的一种示意性框图。

具体实施方式

30 下面将结合附图，详细描述本说明书实施例的技术方案。

本说明书实施例披露一种离线支付的授权方法及装置、离线支付方法及装置、针对离线设备的收款方法及装置，下面首先对离线支付的授权方法的应用场景和发明构思进行介绍，具体如下：

目前使用离线钱包支付的方案，都需要在终端设备处于联网的状态下激活离线钱

包（即开立离线账户）并且“充值”一定数额的钱到离线钱包上，进而，在终端设备处于无网状态下，供用户使用离线钱包提供的离线支付服务。

5 用户往往对提前激活离线钱包并充值的这种操作，没有形成习惯或者事先并不能确定自己需要离线支付服务。在一种示例性场景下：用户乘坐飞机时，其需要买东西，此时，用户的终端设备处于无网状态（离线状态），用户需要使用离线钱包支付服务，需要提前在终端设备联网的情况下把钱“充值”到已激活的离线钱包上。然而，其往往不会提前预料到自己会在飞机上购买东西，从而提前充值离线钱包。相应的，提前激活离线钱包并充值对实际场景应用存在一定程度上的使用限制。

10 鉴于此，本说明书实施例提供了一种离线支付的授权方法，如图 1 所示，为本说明书披露的一个实施例的实施框架示意图，其中，服务器可以针对多个电子钱包账户的当前状态进行检测，如图 1 所示，多个电子钱包账户可以包括电子钱包账户 1、电子钱包账户 2... 电子钱包账户 n，电子钱包账户为电子钱包应用的账户，该电子钱包应用运行于终端设备。电子钱包应用可以包括但不限于支付宝钱包应用、手机钱包应用以及银行终端应用等可以支持在线支付功能的应用。其中，为了支持离线支付功能，15 终端设备还设置有硬件钱包应用，该硬件钱包应用可以以电子钱包应用的插件的形式存在，也可以以独立的客户端软件的形式存在。在硬件钱包应用以独立的客户端软件的形式存在的情况下，电子钱包应用可以与硬件钱包应用绑定，以使得硬件钱包应用可以基于用户证书进行离线支付。一种实现中，该硬件钱包应用可以是基于手机的离线钱包应用，移动、联通等运营商基于手机 SIM 的离线钱包应用，以及各种卡商基于20 支付卡硬件的离线钱包应用。

服务器可以通过其状态检测模块针对电子钱包账户的状态进行检测，如图 1 所示，服务器在检测到电子钱包账户 1 的当前状态满足预设证书下发条件时，将该电子钱包账户 1 作为目标电子钱包账户，通过其第一获得模块获得目标电子钱包账户的钱包账户信息、当前账户余额及当前信用信息；通过其第一确定模块基于当前账户余额以及25 当前信用信息，确定目标电子钱包账户对应的可离线支付额度；通过其第一签名模块利用服务器私钥，对汇总信息进行签名，得到电子钱包签名，汇总信息包括，钱包账户信息、可离线支付额度、签发时间以及有效时长；通过其第一生成模块基于汇总信息以及电子钱包签名，生成目标电子钱包账户对应的用户证书；通过其第一发送模块将用户证书下发至目标电子钱包账户所在终端设备，以使得目标电子钱包账户对应的30 离线账户可基于用户证书在可离线支付额度之内进行离线支付。其中，该离线账户为登录硬件钱包应用的账户，可以通过硬件钱包应用进行离线支付。

一种实现方式中，预设证书下发条件包括如下条件中的至少一个：1、目标电子钱包账户的已获得用户证书过期，且终端设备处于联网状态；2、在已获得用户证书到期之前的第一时段，且终端设备处于联网状态；3、在已获得用户证书到期之前的第二时段，且终端设备的流量使用状态满足预设空闲条件；4、目标电子钱包账户的当前账户35 余额和/或当前信用信息变更达到一定条件；5、目标电子钱包账户未获得过用户证书，且终端设备的流量使用状态满足预设空闲条件。其中，第二时段大于第一时段。

本实施例中，服务器可以基于目标电子钱包账户的当前账户余额以及当前信用信

息，评估出其对应的可离线支付额度，进而生成具有有效期的用户证书，并将用户证书下发至目标电子钱包账户所在终端设备，使得目标电子钱包账户对应的离线账户可基于用户证书在可离线支付额度之内进行离线支付，即通过用户证书实现对离线账户的离线支付授权，使得离线账户无需提前充值即无需提前圈存流动资金，即可实现在可离线支付额度之内的离线支付。并且，在该用户证书为首次针对目标电子钱包账户下发的情况下，还可以实现免开立目标电子钱包账户对应的离线账户（即免激活相应的硬件钱包），实现对该离线账户的免开立及免提前充值的离线支付功能授权。

下面结合具体实施例，对本说明书提供的离线支付的授权方法、离线支付方法、针对离线设备的收款方法进行详细阐述。首先对离线支付的授权方法进行阐述。

- 10 图2示出了本说明书一个实施例中离线支付的授权方法的流程图。该方法可以通过服务器实现，其中，该服务器可以通过任何具有计算、处理能力的装置、设备、平台、设备集群等来实现。所述方法包括如下步骤 S210- S250:

- 15 S210: 在检测到目标电子钱包账户的当前状态满足预设证书下发条件时，获得目标电子钱包账户的钱包账户信息、当前账户余额及当前信用信息。其中，目标电子钱包账户可以是任一当前状态满足预设证书下发条件的电子钱包账户。电子钱包账户为电子钱包应用的账户，该电子钱包应用运行于终端设备。电子钱包应用包括但不限于支付宝钱包应用、手机钱包应用以及银行终端应用等可以支持支付功能的应用。该服务器为电子钱包应用对应的服务器。

- 20 一种实现中，防止目标电子钱包账户的隐私信息的泄露，钱包账户信息可以为：目标电子钱包账户对应的钱包账户 ID 和钱包账户名信息的哈希值。例如，可以为钱包账户 ID 和钱包账户名信息的 MD5 值。该当前信用信息可以表征目标电子钱包账户对应的信用信息，当前信用信息可以包括如下信息中的至少一种：当前的信用值以及当前的可借贷额度。

- 25 一种示例性场景中，电子钱包应用为支付宝钱包应用，目标电子钱包账户为支付宝钱包账户。相应的，钱包账户信息可以为：支付宝钱包账户 ID 和支付宝钱包账户名信息的哈希值；当前账户余额可以为当前的支付宝钱包的用户余额；当前的信用值可以为当前的芝麻信用值；当前的可借贷额度可以为当前的花呗额度。

- 30 在一种实现方式中，预设证书下发条件包括如下条件中的至少一个：1、目标电子钱包账户的已获得用户证书过期，且终端设备处于联网状态；2、在已获得用户证书到期之前的第一时段，且终端设备处于联网状态；3、在已获得用户证书到期之前的第二时段，且终端设备的流量使用状态满足预设空闲条件；4、目标电子钱包账户的当前账户余额和/或当前信用信息变更达到一定条件；5、目标电子钱包账户未获得过用户证书，且终端设备的流量使用状态满足预设空闲条件。其中，第二时段大于第一时段。

- 35 可以理解的是，上述列举的预设证书下发条件仅作为本说明书实施例提供的一种示例，工作人员可以根据实际情况需求设置具体的预设证书下发条件，本说明书实施例并不做限定。例如：该预设证书下发条件还可以包括：目标电子钱包账户未获得过用户证书，其当前的账户余额和/或当前的信用信息满足预设条件（如当前的信用信息

中的当前的信用值超过一定信用值，或者，当前的信用信息中的当前的可借贷额度超过一定额度，或者当前的账户余额不为零等），且终端设备处于联网状态。

在检测到目标电子钱包账户的当前状态满足预设证书下发条件中的任一条件时，均可认为其当前状态满足预设证书下发条件，进而服务器获得该目标电子钱包账户的钱包账户信息、当前账户余额及当前信用信息。

S220：基于当前账户余额以及当前信用信息，确定对应的可离线支付额度。本步骤中，当前账户余额可以在一定程度上表征目标电子钱包账户的可消费能力（当前账户余额越多，可消费能力越大），当前信用信息可以表征目标电子钱包账户的履约程度（当前信用信息中当前的信用值以及当前的可借贷额度越大，履约程度越高），例如其守信还款程度等。鉴于此，基于当前账户余额以及当前信用信息，确定目标电子钱包账户对应的可离线支付额度，该可离线支付额度为：支持目标电子钱包账户对应的离线账户在其所在终端设备在每次联网还款前的可离线支付的最大上限。

S230：利用服务器私钥，对汇总信息进行签名，得到电子钱包签名。汇总信息包括，钱包账户信息、可离线支付额度、签发时间以及有效时长。需要理解，目标电子钱包账户的信用信息以及账户余额的变动，会导致其可消费能力、履约程度变动（例如可消费能力变低或变高），相应的，针对目标电子钱包账户确定的可离线支付额度也会变动。为此，可以针对可离线支付额度（即后续生成用户证书）设置有效期限，具体的可以通过相应的签发时间以及有效时长限制可离线支付额度的有效期限。并且，为了防止汇总信息被篡改，进而导致后续的离线支付过程出现问题，本步骤中，利用服务器私钥，对汇总信息进行签名，得到电子钱包签名。该电子钱包签名用于目标电子钱包账户对应的离线账户进行离线支付时的身份验证以及相应的有效期限验证。

其中，上述签发时间表征用户证书的生成和下发时间。一种情况中，用户证书生成和下发在同一天执行。上述有效时长可以根据经验设置，考虑到目标电子钱包账户相关信息的变更情况以及下发频率情况，上述有效时长可以设置为 3-7 天。

S240：基于汇总信息以及电子钱包签名，生成用户证书。一种实现中，可以将汇总信息以及电子钱包签名组合，生成用户证书。

S250：将用户证书下发至目标电子钱包账户所在终端设备，以使得目标电子钱包账户对应的离线账户可基于用户证书在可离线支付额度之内进行离线支付。在终端设备联网的状态下，服务器将用户证书下发至目标电子钱包账户所在终端设备，终端设备通过所连接的网络，获得并存储该用户证书。后续的，目标电子钱包账户对应的离线账户可基于用户证书进行离线支付。在终端设备联网并进行离线支付清算之前，离线账户进行离线支付的金额上限最高为可离线支付额度，具体的离线支付的金额上限可基于可离线支付额度和历史离线交易金额确定。其中，离线支付清算可以指服务器在终端设备再次联网后，对其离线期间离线账户所产生的离线交易金额进行清算。

在一种实现中，该终端设备安装有硬件钱包应用，以实现离线支付。其中，目标电子钱包账户对应的离线账户为该硬件钱包应用对应的账户。一种情况中，该硬件钱包应用可以以电子钱包应用的插件的形式存在；也可以以独立的客户端应用的形式存

在。在硬件钱包应用以独立的客户端应用的形式存在的情况下，电子钱包应用与该硬件钱包应用绑定，以使得硬件钱包应用可以基于用户证书进行离线支付。

5 本说明书实施例中，通过向目标电子钱包账户所在终端设备下发用户证书，使得目标电子钱包账户对应的离线账户可基于用户证书在可离线支付额度之内进行离线支付。由此，对于离线账户不必提前充值即无需提前圈存流动资金，即可实现在可离线支付额度之内的离线支付。并且，在该用户证书为首次针对目标电子钱包账户下发的情况下，还可以实现免开立目标电子钱包账户对应的离线账户（即免激活相应的硬件钱包），实现对该离线账户的免开立及免提前充值的离线支付功能授权。

10 并且，在本说明书实施例中，对离线账户的免提前充值的离线支付的授权，即不提前将钱圈存于离线账户，不用提前占用用户的流动财产。可以理解的，本实施例中，离线账户可以利用用户证书实现先消费后还款，可以避免在相应的硬件钱包损坏或终端设备丢失时，离线账户内圈存的钱无法找回的问题，避免用户的财产损失。

15 在一种可实施方式中，为了保护用户证书的安全，避免其泄露，终端设备设置有可信执行环境 TEE，相应的，上述 S250，可以包括：将用户证书下发至终端设备的 TEE 中，以使终端设备在 TEE 中存储用户证书。一种情况中，该硬件钱包应用可以安装于终端设备的 TEE 中。

在一种可实施方式中，所述 S220，可以包括如下步骤 11-12：

步骤 11：基于当前账户余额、当前信用信息及其各自对应的权重，确定目标电子钱包账户的账户打分的当前分值。

20 步骤 12：基于当前分值，确定目标电子钱包账户对应的可离线支付额度。

本实现方式中，服务器可以预存有当前账户余额及当前信用信息各自对应的权重，后续的，基于当前账户余额及其对应的权重，和当前信用信息及其对应的权重，确定目标电子钱包账户的账户打分的当前分值。一种情况，可以是当前账户余额及其对应的权重之积，与当前信用信息及其对应的权重之积的和，确定为当前分值；也可以是：首先计算得到当前账户余额及其对应的权重之积，作为第一乘积值，计算得到当前信用信息及其对应的权重之积，作为第二乘积值，将第一乘积值和第二乘积值的平均值作为当前分值。后续的，基于当前分值，确定目标电子钱包账户对应的可离线支付额度。一种情况，服务器预存有分值与额度的映射关系，基于该映射关系，确定当前分值对应的额度，作为可离线支付额度。

30 对于目标电子钱包账户的当前账户余额而言，在目标电子钱包账户的拥有者不断进行消费的情况下，该账户余额会频繁变动。若账户余额一变动，相应的，可离线支付额度即变动，会出现服务器针对目标电子钱包账户频繁生成和下发用户证书，这样既浪费服务器计算资源，又会增多终端设备的网络流程消耗，给用户带来不好的体验。鉴于此，在一种可实施方式中，所述步骤 12，可以包括如下步骤 121-122：

35 步骤 121：基于预设的账户打分与额度等级之间的第一对应关系，确定当前分值对应的当前额度等级。

步骤 122: 基于预设的额度等级与额度值的第二对应关系, 确定当前额度等级对应的额度值, 作为可离线支付额度。

本实现方式中, 划分额度等级, 并且预先构建并存储账户打分与额度等级之间的对应关系及第一对应关系, 以及额度等级与额度值之间的对应关系即第二对应关系。

- 5 后续的, 服务器获得当前分值之后, 基于该第一对应关系, 确定当前分值对应的当前额度等级; 基于该第二对应关系, 确定当前额度等级对应的额度值, 作为可离线支付额度。设置额度等级, 使得仅在当前账户余额和/或当前信用信息变更, 导致计算所得当前分值所对应的额度等级变更时, 才会变更可离线支付额度(变更用户证书), 可以避免服务器针对目标电子钱包账户频繁生成和下发用户证书情况的发生。

- 10 在另一种实现方式中, 可以直接建立账户余额和信用信息, 与额度之间的对应关系, 继而, 基于该对应关系, 确定出当前账户余额和当前信用信息对应的额度, 作为目标电子钱包账户对应的可离线支付额度。

在一种可实施方式中, 所述方法还可以包括如下步骤 21-23:

- 15 步骤 21: 获得终端设备发送的离线账单, 其中, 离线账单为离线账户离线支付生成的账单, 至少包括对应的交易金额以及钱包账户信息。

步骤 22: 基于交易金额以及钱包账户信息, 从目标电子钱包账户中扣除相应的金额。

步骤 23: 发送额度恢复信息至终端设备, 以使离线账户将当前离线支付的上限, 恢复为可离线支付额度。

- 20 本实施方式中, 服务器将用户证书下发至目标电子钱包账户所在终端设备之后, 目标电子钱包账户对应的离线账户可基于用户证书在可离线支付额度之内进行离线支付。离线账户进行离线支付之后, 会生成相应的离线账单, 该离线账单至少包括离线账户进行离线支付对应的交易金额以及钱包账户信息, 以便于终端设备联网之后, 在服务器侧进行离线支付清算。具体的, 终端设备联网之后, 将其在离线期间存储的离线账单, 通过网络上传至服务器。服务器接收离线账单, 并基于其中包括的交易金额以及钱包账户信息, 从目标电子钱包账户中扣除相应的金额, 实现离线支付清算。
- 25

- 可以理解的是, 为了避免离线账户出现双花的情况, 终端设备在离线账户进行一次离线支付后, 会根据其离线支付对应的交易金额, 调整其当前的离线支付的上限。例如, 终端设备获得用户证书之后, 目标电子钱包账户对应的离线账户最初的离线支付的上限为: 用户证书对应的可离线支付额度 300。离线账户进行一次离线支付, 其对应的交易金额为 50, 相应的, 终端设备根据该交易金额 50, 调整离线账户当前离线支付的上限为 250 (300-50); 离线账户再进行一次离线支付, 其对应的交易金额为 100, 相应的, 终端设备根据该交易金额 100, 调整离线账户当前离线支付的上限为 150 (250-100); 以此类推。
- 30

- 35 鉴于此, 为了保证离线账户的离线支付功能的正常使用, 服务器进行清算之后, 发送额度恢复信息至终端设备。终端设备获得该额度恢复信息之后, 恢复离线账户的

离线支付的上限，即将离线账户的当前离线支付的上限，恢复为可离线支付额度。

- 5 在一种情况中，可能会出现终端设备在离线期间，目标电子钱包账户对应的离线账户的用户证书出现过期的情况，针对这种情况，服务器针对该离线账户进行离线支付清算即执行完成步骤 22 之后，可以直接针对目标电子钱包账户重新生成新的用户证书，不再执行步骤 23。也就是说，服务器针对该离线账户进行清算之后，可以先确定离线账户当前已获得的用户证书是否过期，在确定离线账户当前已获得的用户证书未过期的情况下，执行步骤 23。

- 10 在一种可实施方式中，为了防止离线账单被篡改或伪造，该离线账单还可以包括：相应的商户账户信息以及商户签名，商户签名为：利用商户私钥对商户账户信息以及交易金额签名所得；其中，该相应的商户账户信息为：离线账户进行离线支付对应的商家的账户信息。

所述步骤 22，可以包括如下步骤 221-222：

步骤 221：利用商户私钥对应的商户公钥，对离线账单进行验证。

- 15 步骤 222：若验证通过，基于交易金额以及钱包账户信息，从目标电子钱包账户中扣除相应的金额。

- 20 本实现方式中，服务器可以利用商户私钥对应的商户公钥，对离线账单进行验证，确定该离线账单是否被篡改，在验证通过即确定离线账单未被篡改的情况下，则基于交易金额以及钱包账户信息，从目标电子钱包账户中扣除相应的金额。若验证不通过，则可以确定离线账单被篡改，服务器锁定该离线账单，并进行后续的特定处理操作。该特定处理操作例如可以为：服务器通过查询相应商户对应的交易记录，对该离线账单进行核实。

- 25 相应于上述方法实施例，本说明书实施例还提供了一种离线支付方法，应用于终端设备，终端设备存储有服务器下发的用户证书，用户证书至少包括，可离线支付额度、签发时间、有效时长以及电子钱包签名，如图 3 所示，所述方法可以包括步骤 S310-S340：

- 30 S310：在接收到离线支付指令的情况下，判断离线支付指令携带的当前交易金额是否不大于当前离线支付的上限。其中，当前离线支付的上限基于可离线支付额度以及历史离线交易金额确定。一种情况中，当前离线支付的上限可以为：可离线支付额度与所有历史离线交易金额的差值。历史离线交易金额包括：终端设备在最近一次恢复或确定该可离线支付额度之后，本次离线支付之前，所进行的历史离线支付对应的交易金额。

- 35 一种示例性的离线支付场景中，终端设备可以通过扫描商户出示的收款码的方式，接收到离线支付指令，其中，该收款码中包含该当前交易金额。另一种示例性的离线支付场景中，终端设备可以根据用户操作接收到离线支付指令，例如：用户操作可以是在指定支付界面输入当前交易金额，以使得终端设备接收到离线支付指令。另一种示例性的离线支付场景中，终端设备可以基于用户操作出示付款码，以供收款设备扫

描，收款设备扫描终端设备出示的付款码之后，可以向终端设备提供当前交易金额，相应的，终端设备获得该当前交易金额，则认为获得离线支付指令。

- 5 在一种实现中，终端设备可以安装有硬件钱包应用，终端设备通过该硬件钱包应用实现离线支付功能。在另一种实现中，终端设备还安装有电子钱包应用。该硬件钱包应用可以以电子钱包应用的插件的形式存在；也可以以独立的客户端应用的形式存在。在硬件钱包应用以独立的客户端应用的形式存在的情况下，电子钱包应用与该硬件钱包应用绑定，以使得该硬件钱包应用可以基于用户证书进行离线支付。

- 10 上述服务器为电子钱包应用对应的服务器，终端设备可以通过电子钱包应用获得用户证书。上述可离线支付额度是基于电子钱包应用所登录的电子钱包账户的账户余额以及信用信息确定的。上述用户证书还可以包括电子钱包账户的钱包账户信息。该钱包账户信息可以证明用户证书所属账户。上述电子钱包签名为：基于服务器私钥对钱包账户信息、可离线支付额度、签发时间以及有效时长进行签名所得。签发时间可以包括用户证书生成和下发的时间，有效时长可以限制用户证书的有效期限。

- 15 S320：若判断当前交易金额不大于当前离线支付的上限，将用户证书提供至离线支付指令对应的收款设备。本步骤中，终端设备若判断当前交易金额不大于当前离线支付的上限，则认为该次交易可以进行，相应的，将用户证书提供至离线支付指令对应的收款设备。一种实现中，终端设备可以通过短距离传输方式，将用户证书提供至离线支付指令对应的收款设备。该短距离传输方式可以包括但不限于：蓝牙传输方式，扫码传输方式，基于 NFC（Near Field Communication，近场通信）技术的传输方式。

- 20 S330：获得收款设备提供的交易确认信息。其中，交易确认信息为收款设备基于电子钱包签名确定用户证书有效的情况下发送的。

S340：基于交易确认信息生成离线账单。

- 25 终端设备将用户证书提供至收款设备之后，收款设备基于电子钱包签名对用户证书进行验证，在用户证书验证通过即确定用户证书有效之后，进行交易。收款设备进行交易之后，生成交易确认信息并向终端设备提供该交易确认信息，以通知终端设备该次交易（离线支付）成功。终端设备获得收款设备提供的交易确认信息，并基于该交易确认信息生成离线账单。服务器可以通过离线账单对离线账户进行离线支付清算。

一种情况中，收款设备可以通过上述短距离传输方式，向终端设备提供交易确认信息。

- 30 本实施例中，终端设备可以在确定当前离线支付的上限大于当前交易金额，即可支付当前交易金额时，将用户证书提供至收款设备，即通过用户证书实现离线支付。

- 35 在一种可实施方式中，为了避免用户证书被窃取或篡改，终端设备可以包括可信执行环境 TEE，用户证书可以存储在 TEE 中，该离线支付方法在 TEE 中执行。相应的，避免硬件钱包应用被恶意破坏，上述硬件钱包应用可以安装并运行于 TEE 中。考虑到 TEE 的空间资源的有限性，电子钱包应用可以运行于终端设备的通用执行环境 REE 中。

在一种可实施方式中，所述方法还可以包括如下步骤 31-32：

步骤 31：基于离线支付指令的接收时间、用户证书的签发时间及有效时长，判断用户证书是否有效；

在确定用户证书有效的情况下，将用户证书提供至离线支付指令对应的收款设备。

- 5 一种实现方式中，终端设备在确定当前交易金额不大于当前离线支付的上限的情况下，可以执行步骤 31，基于离线支付指令的接收时间、用户证书的签发时间及有效时长，判断用户证书是否有效，即判断签发时间加上有效时长之后对应的时间，是否不早于接收时间。在判断签发时间加上有效时长之后对应的时间，不早于接收时间的情况下，则确定用户证书有效，通过短距离传输方式，将用户证书提供至离线支付指令对应的收款设备。通过该实现方式，可以避免终端设备与收款设备的无效交互，例如：在确定用户证书无效时，终端设备不将用户证书提供至收款设备，直接得到无法进行离线支付的结果。
- 10

- 另一种实现方式中，终端设备也可以在接收到离线支付指令后，首先基于离线支付指令的接收时间、用户证书的签发时间及有效时长，判断用户证书是否有效，在判断用户证书有效的情况下，判断离线支付指令携带的当前交易金额是否不大于当前离线支付的上限，进而，在判断当前交易金额不大于当前离线支付的上限的情况下，将用户证书提供至离线支付指令对应的收款设备。若判断用户证书无效，则不再执行后续步骤。
- 15

- 为了避免离线账户的双花问题，终端设备在获得收款设备提供的交易确认信息，即确定本次离线支付成功的情况下，需要更新其当前离线支付的上限。相应的，在一种可实施方式中，所述方法还可以包括如下步骤 41-42：
- 20

步骤 41：计算当前离线支付的上限与当前交易金额的差值。

步骤 42：将差值确定为新的当前离线支付的上限。

- 本说明书实施例中，终端设备在离线期间基于用户证书进行离线支付生成的离线账单，会保存于终端设备本地，为了避免离线账单被篡改，可以将离线账单存储于 TEE 中。后续的，为了保证离线账户的正常使用，在终端设备再次连接网络的情况下，将离线账单上传至服务器，服务器基于离线账单对离线账户进行清算。
- 25

- 一种实现，终端设备在检测到其自身处于联网状态下，可以自动检索本地存储的所有未上传服务器的离线账单，并自动将所有离线账单发送至服务器。另一种实现，终端设备在检测到其自身处于联网状态下，自动检索本地存储的所有未上传服务器的离线账单，并显示离线账单提示信息，以提示用户上传离线账单，之后在接收到用户的离线账单上传指令的情况下，将离线账单发送至服务器。
- 30

- 相应的，所述方法还可以包括如下步骤：在处于联网状态下，将离线账单发送至服务器，以使服务器基于离线账单进行清算。后续的，服务器进行清算之后，可以继续判断离线账户已获得的用户证书是否有效，在确定用户证书有效的情况下，向终端设备发送额度恢复信息。终端设备获得该额度恢复信息之后，将当前离线支付的上限，
- 35

恢复为用户证书携带的可离线支付额度。

为了避免交易确认信息造假，或者被篡改，终端设备获得交易确认信息之后，可以首先针对交易确认信息进行验证，相应的，在一种可实施方式中，交易确认信息包括：商户的商户账户信息、当前交易金额以及商户签名，商户签名为：利用商户私钥对商户账户信息以及当前交易金额签名所得；

所述 S340，可以包括如下步骤 51-52：

步骤 51：基于商户私钥对应的商户公钥，对交易确认信息进行验证；

步骤 52：若验证通过，基于商户账户信息、当前交易金额以及钱包账户信息，生成离线账单。

其中，该商户私钥对应的商户公钥可以是被预存于终端设备本地的，或者也可以是在终端设备与商户进行交易时，收款设备将其提供给终端设备的。终端设备获得交易确认信息之后，基于商户私钥对应的商户公钥，对交易确认信息进行验证，若验证通过即确定交易确认信息中商户账户信息和当前交易金额均未被篡改，基于商户账户信息、当前交易金额以及钱包账户信息，生成离线账单。该离线账单可以至少包括商户账户信息、当前交易金额以及钱包账户信息。

另一种实现中，该离线账单中还可以包括该商户签名，以使得服务器在对离线账户进行清算之前，先利用商户私钥对应的商户公钥，对离线账单进行验证，以验证离线账单携带的商户账户信息和交易金额是否被篡改，服务器在确定离线账单携带的商户账户信息和交易金额未被篡改即对离线账单验证通过之后，再针对离线账户进行清算，即基于交易金额以及离线账单携带的钱包账户信息，从相应的电子钱包账户中扣除相应的金额。以避免电子钱包账户的财产损失。

相应于上述方法实施例，本说明书实施例还提供了一种针对离线设备的收款方法，应用于收款设备，如图 4 所示，所述方法包括如下步骤 S410-S450：

S410：获得离线的终端设备提供的用户证书。其中，用户证书由服务器下发，并包括：终端设备对应的电子钱包账户的钱包账户信息、可离线支付金额、用户证书的签发时间和有效时长以及电子钱包签名。

该用户证书为基于上述实施例中所提供的离线支付的授权方法所生成的用户证书，具体生成过程可以参见上述离线支付的授权方法实施例，在此不再赘述。该用户证书由服务器生成并下发至处于联网状态的终端设备。终端设备将其存储于本地，例如存储于终端设备的可信执行环境 TEE 中。后续的，终端设备处于离线状态下，可以基于该用户证书进行离线支付，即与商户进行离线交易。

在一种情况中，在该终端设备处于离线状态下与商户进行交易（进行离线支付）时，可以通过短距离传输方式将用户证书提供至该商户的收款设备，收款设备通过短距离传输方式获得离线的终端设备提供的用户证书。其中，短距离传输方式可以包括但不限于：蓝牙通信方式，扫码通信方式，基于 NFC（Near Field Communication，近场通信）技术的传输方式。

S420: 利用服务器的公钥, 对电子钱包签名进行验证。其中, 该电子钱包签名为: 利用该服务器的私钥 (即上述实施例所提的服务器私钥), 对终端设备对应的电子钱包账户的钱包账户信息、可离线支付金额、用户证书的签发时间和有效时长进行签名所生成的。该服务器的公钥可以被预先存储于收款设备本地, 或者也可以在收款设备
5 获得该用户证书之后, 从服务器处下载所得。

收款设备利用服务器的公钥, 对电子钱包签名进行验证, 以验证用户证书中钱包账户信息、可离线支付金额、用户证书的签发时间和有效时长是否被篡改, 在确定钱包账户信息、可离线支付金额、用户证书的签发时间和有效时长均未被篡改, 即确定电子钱包签名验证通过, 相应的, 执行后续步骤 S430。若确定钱包账户信息、可离线
10 支付金额、用户证书的签发时间和有效时长任一信息被篡改, 则确定电子钱包签名验证失败, 无法进行交易。

在一种实现方式中, 收款设备在确定电子钱包签名验证失败之后, 可以向终端设备提供表征交易失败的信息。或者, 收款设备在确定电子钱包签名验证失败之后, 可以在其连接的显示屏幕上显示表征用户证书有误的信息, 收款设备使用者可以基于该
15 信息确定交易付款失败, 继而执行相应操作。例如提醒终端设备用户无法进行支付, 建议其更换其他支付方式。

S430: 若验证通过, 基于本次交易的交易时间、签发时间及有效时长, 判断用户证书是否有效。本步骤中, 在确定电子钱包签名验证通过之后, 收款设备获取本次交易的交易时间, 基于该交易时间、签发时间及有效时长, 判断用户证书是否有效。

20 其中, 判断用户证书是否有效的过程, 可以是: 基于签发时间和有效时长确定第一时间, 判断该交易时间是否不晚于该第一时间。后续的, 在判断该交易时间不晚于该第一时间, 判断用户证书有效; 反之, 在判断该交易时间晚于该第一时间, 判断用户证书无效。

S440: 在判断用户证书有效的情况下, 生成本次交易相应的交易确认信息。本步骤中, 收款设备在判断用户证书有效的情况下, 进行交易, 并生成本次交易相应的交易确认信息。其中, 该交易确认信息用于表征本次交易成功。在一种情况中, 交易确认信息至少可以包括: 商户的商户账户信息、本次交易的交易金额以及商户签名, 商户签名为: 利用商户私钥至少对商户账户信息以及当前交易金额签名所得。后续的, 终端设备侧和/或服务
25 器侧, 可以通过商户签名验证商户账户信息以及当前交易金额是否被篡改。

在另一种实现方式中, 在判断用户证书无效的情况下, 收款设备可以生成交易失败信息; 将交易失败信息提供至终端设备。或者, 收款设备在判断用户证书无效之后, 可以在其连接的显示屏幕上显示表征用户证书无效的信息, 收款设备使用者可以基于该信息确定交易付款失败, 继而执行相应操作。例如提醒终端设备用户无法进行支付,
35 建议其更换其他支付方式。

S450: 将交易确认信息提供至终端设备, 以使终端设备基于交易确认信息生成相应的离线账单。在一种实现方式中, 收款设备生成交易确认信息之后, 可以通过短距

离传输方式，将交易确认信息提供至终端设备，终端设备获得交易确认信息之后，基于交易确认信息生成相应的离线账单。

本实施例中，收款设备在验证终端设备提供的用户证书有效的情况下，进行交易，为终端设备在离线状态下的交易提供便利。

5 上述内容对本说明书的特定实施例进行了描述，其他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按照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。

10 相应于上述方法实施例，本说明书实施例，提供了一种离线支付的授权装置 500，应用于服务器，其示意性框图如图 5 所示，所述装置包括：

第一获得模块 510，配置为在检测到目标电子钱包账户的当前状态满足预设证书下发条件时，获得所述目标电子钱包账户的钱包账户信息、当前账户余额及当前信用信息；

15 第一确定模块 520，配置为基于所述当前账户余额以及所述当前信用信息，确定对应的可离线支付额度；

第一签名模块 530，配置为利用服务器私钥，对汇总信息进行签名，得到电子钱包签名，所述汇总信息包括，所述钱包账户信息、所述可离线支付额度、签发时间以及有效时长；

20 第一生成模块 540，配置为基于所述汇总信息以及所述电子钱包签名，生成用户证书；

第一发送模块 550，配置为将所述用户证书下发至所述目标电子钱包账户所在终端设备，以使得所述目标电子钱包账户对应的离线账户可基于所述用户证书在所述可离线支付额度之内进行离线支付。

25 在一种可实施方式中，所述预设证书下发条件包括如下条件中的至少一个：所述目标电子钱包账户的已获得用户证书过期，且所述终端设备处于联网状态；

在所述已获得用户证书到期之前的第一时段，且所述终端设备处于联网状态；

在所述已获得用户证书到期之前的第二时段，且所述终端设备的流量使用状态满足预设空闲条件；

30 所述目标电子钱包账户的当前账户余额和/或所述当前信用信息变更达到一定条件；

所述目标电子钱包账户未获得过用户证书，且所述终端设备的流量使用状态满足预设空闲条件。

35 在一种可实施方式中，所述钱包账户信息为：所述目标电子钱包账户对应的钱包账户 ID 和钱包账户名信息的哈希值。

在一种可实施方式中，所述当前信用信息包括如下信息中的至少一种：当前的信用值以及当前的可借贷额度。

在一种可实施方式中，所述终端设备设置有可信执行环境 TEE；

5 所述第一发送模块 550，具体配置为将所述用户证书下发至所述终端设备的 TEE 中，以使所述终端设备在所述 TEE 中存储所述用户证书。

在一种可实施方式中，所述第一确定模块 520，包括：

第一确定单元（图中未示出），配置为基于所述当前账户余额、所述当前信用信息及其各自对应的权重，确定所述目标电子钱包账户的账户打分的当前分值；

10 第二确定单元（图中未示出），配置为基于所述当前分值，确定所述目标电子钱包账户对应的可离线支付额度。

在一种可实施方式中，所述第二确定单元，具体配置为基于预设的账户打分与额度等级之间的第一对应关系，确定所述当前分值对应的当前额度等级；

基于预设的额度等级与额度值的第二对应关系，确定所述当前额度等级对应的额度值，作为所述可离线支付额度。

15 在一种可实施方式中，所述装置还包括：

第四获得模块（图中未示出），配置为获得所述终端设备发送的离线账单，其中，所述离线账单为所述离线账户离线支付生成的账单，至少包括对应的交易金额以及所述钱包账户信息；

20 金额扣除模块（图中未示出），配置为基于所述交易金额以及所述钱包账户信息，从所述目标电子钱包账户中扣除相应的金额；

第二发送模块（图中未示出），配置为发送额度恢复信息至所述终端设备，以使所述离线账户的当前离线支付的上限，恢复为所述可离线支付额度。

在一种可实施方式中，所述离线账单还包括：相应的商户账户信息以及商户签名，所述商户签名为：利用商户私钥对所述商户账户信息以及所述交易金额签名所得；

25 所述金额扣除模块，具体配置为利用所述商户私钥对应的商户公钥，对所述离线账单进行验证；

若验证通过，基于所述交易金额以及所述钱包账户信息，从所述目标电子钱包账户中扣除相应的金额。

30 相应于上述方法实施例，本说明书实施例，提供了一种离线支付装置 600，应用于终端设备，所述终端设备存储有服务器下发的用户证书，所述用户证书至少包括，可离线支付额度、签发时间、有效时长以及电子钱包签名，其示意性框图如图 6 所示，所述装置包括：

第一判断模块 610，配置为在接收到离线支付指令的情况下，判断所述离线支付指令携带的当前交易金额是否不大于当前离线支付的上限，其中，所述当前离线支付

的上限基于所述可离线支付额度以及历史离线交易金额确定；

第一提供模块 620，配置为若判断所述当前交易金额不大于所述当前离线支付的上限，将所述用户证书提供至所述离线支付指令对应的收款设备；

- 5 第二获得模块 630，配置为获得所述收款设备提供的交易确认信息，其中，所述交易确认信息为所述收款设备基于所述电子钱包签名确定所述用户证书有效的情况下发送的；

第二生成模块 640，配置为基于所述交易确认信息生成离线账单。

在一种可实施方式中，所述终端设备包括可信执行环境 TEE，所述用户证书存储于所述 TEE 中，所述方法在所述 TEE 中执行。

- 10 在一种可实施方式中，所述装置还包括：

第三判断模块（图中未示出），配置为基于所述离线支付指令的接收时间、所述用户证书的签发时间及有效时长，判断所述用户证书是否有效；

第三提供模块（图中未示出），配置为在确定所述用户证书有效的情况下，将所述用户证书提供至所述收款设备。

- 15 在一种可实施方式中，所述装置还包括：

计算模块（图中未示出），配置为计算所述当前离线支付的上限与所述当前交易金额的差值；

第二确定模块（图中未示出），配置为将所述差值确定为新的当前离线支付的上限。

- 20 在一种可实施方式中，所述装置还包括：

第三发送模块（图中未示出），配置为在处于联网状态下，将所述离线账单发送至所述服务器，以使所述服务器基于所述离线账单进行清算。

在一种可实施方式中，所述第二获得模块 630，具体配置为通过短距离传输方式，获得所述收款设备提供的交易确认信息。

- 25 在一种可实施方式中，所述交易确认信息包括：所述商户的商户账户信息、所述当前交易金额以及商户签名，所述商户签名为：利用商户私钥对所述商户账户信息以及所述当前交易金额签名所得；

所述第二生成模块 640，具体配置为基于所述商户私钥对应的商户公钥，对所述交易确认信息进行验证；

- 30 若验证通过，基于所述商户账户信息、所述当前交易金额以及所述钱包账户信息，生成离线账单。

相应于上述方法实施例，本说明书实施例，提供了一种针对离线设备的收款装置 700，应用于收款设备，其示意性框图如图 7 所示，所述装置包括：

第三获得模块 710，配置为获得离线的终端设备提供的用户证书，其中，所述用户证书由服务器下发，并包括：所述终端设备对应的电子钱包账户的钱包账户信息、可离线支付金额、所述用户证书的签发时间和有效时长以及电子钱包签名；

5 第一验证模块 720，配置为利用所述服务器的公钥，对所述电子钱包签名进行验证；

第二判断模块 730，配置为若验证通过，基于本次交易的交易时间、所述签发时间及所述有效时长，判断所述用户证书是否有效；

第三生成模块 740，配置为在判断所述用户证书有效的情况下，生成本次交易相应的交易确认信息；

10 第二提供模块 750，配置为将所述交易确认信息提供至所述终端设备，以使所述终端设备基于所述交易确认信息生成相应的离线账单

在一种可实施方式中，所述交易确认信息至少包括：所述商户的商户账户信息、本次交易的交易金额以及商户签名，所述商户签名为：利用商户私钥对所述商户账户信息以及所述当前交易金额签名所得。

15 在一种可实施方式中，所述第二提供模块 750，具体配置为通过短距离传输方式，将所述交易确认信息提供至所述终端设备。

在一种可实施方式中，所述装置还包括：

第四生成模块（图中未示出），配置为在判断所述用户证书无效的情况下，生成交易失败信息；

20 第四提供模块（图中未示出），配置为将所述交易失败信息提供至所述终端设备。

上述装置实施例与方法实施例相对应，具体说明可以参见方法实施例部分的描述，此处不再赘述。装置实施例是基于对应的方法实施例得到，与对应的方法实施例具有同样的技术效果，具体说明可参见对应的方法实施例。

25 本说明书实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行本说明书所提供的所述离线支付的授权方法。

本说明书实施例还提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书所提供的所述离线支付的授权方法。

30 本说明书实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行本说明书所提供的所述离线支付方法。

35 本说明书实施例还提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书所提供的所述离线支付方法。

本说明书实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行本说明书所提供的所述针对离线设备的收款方法。

- 5 本说明书实施例还提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书所提供的所述针对离线设备的收款方法。

- 10 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，对于存储介质和计算设备实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。

- 15 本领域技术人员应该可以意识到，在上述一个或多个示例中，本说明书实施例所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

- 20 以上所述的具体实施方式，对本发明实施例的目的、技术方案和有益效果进行了进一步的详细说明。所应理解的是，以上所述仅为本说明书实施例的具体实施方式而已，并不用于限定本说明书的保护范围，凡在本说明书的技术方案的基础之上所做的任何修改、等同替换、改进等，均应包括在本说明书的保护范围之内。

权 利 要 求 书

- 1、一种离线支付的授权方法，应用于服务器，所述方法包括：

在检测到目标电子钱包账户的当前状态满足预设证书下发条件时，获得所述目标电子钱包账户的钱包账户信息、当前账户余额及当前信用信息；

基于所述当前账户余额以及所述当前信用信息，确定对应的可离线支付额度；

利用服务器私钥，对汇总信息进行签名，得到电子钱包签名，所述汇总信息包括，所述钱包账户信息、所述可离线支付额度、签发时间以及有效时长；

基于所述汇总信息以及所述电子钱包签名，生成用户证书；

将所述用户证书下发至所述目标电子钱包账户所在终端设备，以使得所述目标电子钱包账户对应的离线账户可基于所述用户证书在所述可离线支付额度之内进行离线支付。
- 2、根据权利要求1所述的方法，其中，所述预设证书下发条件包括如下条件中的至少一个：所述目标电子钱包账户的已获得用户证书过期，且所述终端设备处于联网状态；

在所述已获得用户证书到期之前的第一时段，且所述终端设备处于联网状态；

在所述已获得用户证书到期之前的第二时段，且所述终端设备的流量使用状态满足预设空闲条件；

所述目标电子钱包账户的当前账户余额和/或所述当前信用信息变更达到一定条件；

所述目标电子钱包账户未获得过用户证书，且所述终端设备的流量使用状态满足预设空闲条件。
- 3、根据权利要求1所述的方法，其中，所述钱包账户信息为：所述目标电子钱包账户对应的钱包账户ID和钱包账户名信息的哈希值。
- 4、根据权利要求1所述的方法，其中，所述当前信用信息包括如下信息中的至少一种：当前的信用值以及当前的可借贷额度。
- 5、根据权利要求1所述的方法，其中，所述终端设备设置有可信执行环境TEE；

所述将所述用户证书下发至所述目标电子钱包账户所在终端设备，包括：

将所述用户证书下发至所述终端设备的TEE中，以使所述终端设备在所述TEE中存储所述用户证书。
- 6、根据权利要求1所述的方法，其中，所述基于所述当前账户余额以及所述当前信用信息，确定对应的可离线支付额度，包括：

基于所述当前账户余额、所述当前信用信息及其各自对应的权重，确定所述目标

电子钱包账户的账户打分的当前分值；

基于所述当前分值，确定所述目标电子钱包账户对应的可离线支付额度。

7、根据权利要求6所述的方法，其中，所述基于所述当前分值，确定所述目标电子钱包账户对应的可离线支付额度，包括：

基于预设的账户打分与额度等级之间的第一对应关系，确定所述当前分值对应的当前额度等级；

基于预设的额度等级与额度值的第二对应关系，确定所述当前额度等级对应的额度值，作为所述可离线支付额度。

8、根据权利要求1-7任一项所述的方法，还包括：

获得所述终端设备发送的离线账单，其中，所述离线账单为所述离线账户离线支付生成的账单，至少包括对应的交易金额以及所述钱包账户信息；

基于所述交易金额以及所述钱包账户信息，从所述目标电子钱包账户中扣除相应的金额；

发送额度恢复信息至所述终端设备，以使所述离线账户的当前离线支付的上限，恢复为所述可离线支付额度。

9、根据权利要求8所述的方法，其中，所述离线账单还包括：相应的商户账户信息以及商户签名，所述商户签名为：利用商户私钥对所述商户账户信息以及所述交易金额签名所得；

所述基于所述交易金额以及所述钱包账户信息，从所述目标电子钱包账户中扣除相应的金额，包括：

利用所述商户私钥对应的商户公钥，对所述离线账单进行验证；

若验证通过，基于所述交易金额以及所述钱包账户信息，从所述目标电子钱包账户中扣除相应的金额。

10、一种离线支付方法，应用于终端设备，所述终端设备存储有服务器下发的用户证书，所述用户证书至少包括，可离线支付额度、签发时间、有效时长以及电子钱包签名，所述方法包括：

在接收到离线支付指令的情况下，判断所述离线支付指令携带的当前交易金额是否不大于当前离线支付的上限，其中，所述当前离线支付的上限基于所述可离线支付额度以及历史离线交易金额确定；

若判断所述当前交易金额不大于所述当前离线支付的上限，将所述用户证书提供至所述离线支付指令对应的收款设备；

获得所述收款设备提供的交易确认信息，其中，所述交易确认信息为所述收款设备基于所述电子钱包签名确定所述用户证书有效的情况下发送的；

基于所述交易确认信息生成离线账单。

11、根据权利要求 10 所述的方法，其中，所述终端设备包括可信执行环境 TEE，所述用户证书存储在所述 TEE 中，所述方法在所述 TEE 中执行。

12、根据权利要求 10 所述的方法，还包括：

基于所述离线支付指令的接收时间、所述用户证书的签发时间及有效时长，判断所述用户证书是否有效；

在确定所述用户证书有效的情况下，将所述用户证书提供至所述收款设备。

13、根据权利要求 10 所述的方法，还包括：

计算所述当前离线支付的上限与所述当前交易金额的差值；

将所述差值确定为新的当前离线支付的上限。

14、根据权利要求 10 所述的方法，还包括：

在处于联网状态下，将所述离线账单发送至所述服务器，以使所述服务器基于所述离线账单进行清算。

15、根据权利要求 10 所述的方法，其中，所述获得所述收款设备提供的交易确认信息，包括：

通过短距离传输方式，获得所述收款设备提供的交易确认信息。

16、根据权利要求 10 所述的方法，其中，所述交易确认信息包括：所述商户的商户账户信息、所述当前交易金额以及商户签名，所述商户签名为：利用商户私钥对所述商户账户信息以及所述当前交易金额签名所得；

所述基于所述交易确认信息生成离线账单，包括：

基于所述商户私钥对应的商户公钥，对所述交易确认信息进行验证；

若验证通过，基于所述商户账户信息、所述当前交易金额以及所述钱包账户信息，生成离线账单。

17、一种针对离线设备的收款方法，应用于收款设备，所述方法包括：

获得离线的终端设备提供的用户证书，其中，所述用户证书由服务器下发，并包括：所述终端设备对应的电子钱包账户的钱包账户信息、可离线支付金额、所述用户证书的签发时间和有效时长以及电子钱包签名；

利用所述服务器的公钥，对所述电子钱包签名进行验证；

若验证通过，基于本次交易的交易时间、所述签发时间及所述有效时长，判断所述用户证书是否有效；

在判断所述用户证书有效的情况下，生成本次交易相应的交易确认信息；

将所述交易确认信息提供至所述终端设备，以使所述终端设备基于所述交易确认信息生成相应的离线账单。

18、根据权利要求 17 所述的方法，其中，所述交易确认信息至少包括：所述商户的商户账户信息、本次交易的交易金额以及商户签名，所述商户签名为：利用商户私钥对所述商户账户信息以及所述当前交易金额签名所得。

19、根据权利要求 17 所述的方法，其中，所述将所述交易确认信息提供至所述终端设备，包括：

通过短距离传输方式，将所述交易确认信息提供至所述终端设备。

20、根据权利要求 17 所述的方法，还包括：

在判断所述用户证书无效的情况下，生成交易失败信息；

将所述交易失败信息提供至所述终端设备。

21、一种离线支付的授权装置，应用于服务器，所述装置包括：

第一获得模块，配置为在检测到目标电子钱包账户的当前状态满足预设证书下发条件时，获得所述目标电子钱包账户的钱包账户信息、当前账户余额及当前信用信息；

第一确定模块，配置为基于所述当前账户余额以及所述当前信用信息，确定对应的可离线支付额度；

第一签名模块，配置为利用服务器私钥，对汇总信息进行签名，得到电子钱包签名，所述汇总信息包括，所述钱包账户信息、所述可离线支付额度、签发时间以及有效时长；

第一生成模块，配置为基于所述汇总信息以及所述电子钱包签名，生成用户证书；

第一发送模块，配置为将所述用户证书下发至所述目标电子钱包账户所在终端设备，以使得所述目标电子钱包账户对应的离线账户可基于所述用户证书在所述可离线支付额度之内进行离线支付。

22、一种离线支付装置，应用于终端设备，所述终端设备存储有服务器下发的用户证书，所述用户证书至少包括，可离线支付额度、签发时间、有效时长以及电子钱包签名，所述装置包括：

第一判断模块，配置为在接收到离线支付指令的情况下，判断所述离线支付指令携带的当前交易金额是否不大于当前离线支付的上限，其中，所述当前离线支付的上限基于所述可离线支付额度以及历史离线交易金额确定；

第一提供模块，配置为若判断所述当前交易金额不大于所述当前离线支付的上限，将所述用户证书提供至所述离线支付指令对应的收款设备；

第二获得模块，配置为获得所述收款设备提供的交易确认信息，其中，所述交易确认信息为所述收款设备基于所述电子钱包签名确定所述用户证书有效的情况下发送的；

第二生成模块，配置为基于所述交易确认信息生成离线账单。

23、一种针对离线设备的收款装置，应用于收款设备，所述装置包括：

第三获得模块，配置为获得离线的终端设备提供的用户证书，其中，所述用户证书由服务器下发，并包括：所述终端设备对应的电子钱包账户的钱包账户信息、可离线支付金额、所述用户证书的签发时间和有效时长以及电子钱包签名；

第一验证模块，配置为利用所述服务器的公钥，对所述电子钱包签名进行验证；

第二判断模块，配置为若验证通过，基于本次交易的交易时间、所述签发时间及所述有效时长，判断所述用户证书是否有效；

第三生成模块，配置为在判断所述用户证书有效的情况下，生成本次交易相应的交易确认信息；

第二提供模块，配置为将所述交易确认信息提供至所述终端设备，以使所述终端设备基于所述交易确认信息生成相应的离线账单。

24、一种计算设备，包括存储器和处理器，其中，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-9 或 10-16 或 17-20 中任一项所述的方法。