

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 1 月 26 日 (26.01.2017)



(10) 国际公布号
WO 2017/012223 A1

- (51) 国际专利分类号:
G06Q 20/32 (2012.01) G06Q 20/40 (2012.01)
- (21) 国际申请号: PCT/CN2015/094730
- (22) 国际申请日: 2015 年 11 月 16 日 (16.11.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510425221.8 2015 年 7 月 17 日 (17.07.2015) CN
- (71) 申请人: 百度在线网络技术(北京)有限公司
(BAIDU ONLINE NETWORK TECHNOLOGY
(BEIJING) CO., LTD.) [CN/CN]; 中国北京市海淀区
上地十街 10 号百度大厦, Beijing 100085 (CN)。
- (72) 发明人: 王晓航 (WANG, Xiaohang); 中国北京市海
淀区上地十街 10 号百度大厦, Beijing 100085 (CN)。
林雪涛 (LIN, Xuetao); 中国北京市海淀区上地十街
10 号百度大厦, Beijing 100085 (CN)。董扬 (DONG,
Yang); 中国北京市海淀区上地十街 10 号百度大厦,
Beijing 100085 (CN)。鲁娜 (LU, Na); 中国北京市
海淀区上地十街 10 号百度大厦, Beijing 100085
(CN)。毛洪博 (MAO, Hongbo); 中国北京市海淀区
上地十街 10 号百度大厦, Beijing 100085 (CN)。

(74) 代理人: 北京汉昊知识产权代理事务所(普通合
伙) (HANHOW INTELLECTUAL PROPERTY); 中
国北京市东长安街 1 号东方广场西 1 区 1111 室,
Beijing 100738 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保
护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,
BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR,
CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,
JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU,
LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA,
RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST,
SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保
护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA,
RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ,
BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH,
CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE,
IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,
RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) Title: NFC-BASED MOBILE PAYMENT METHOD AND DEVICE

(54) 发明名称: 基于 NFC 的移动支付方法和装置

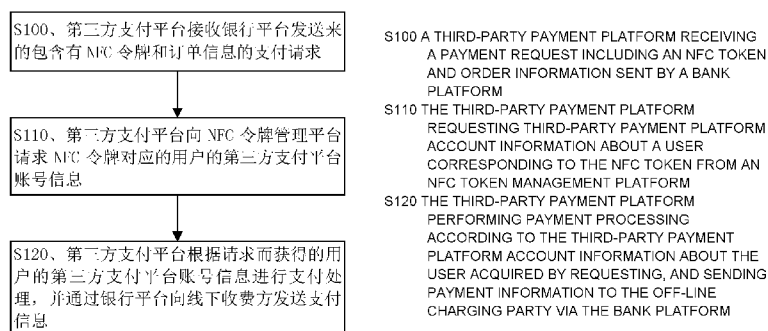


图 1

(57) Abstract: Provided are an NFC-based mobile payment method and device. The method comprises: a third-party payment platform receiving a payment request containing an NFC token and order information sent by a bank platform, wherein the NFC token is transmitted to an off-line charging party by a mobile device of a user, and the NFC token and the order information are transmitted to the bank platform by the off-line charging party; the third-party payment platform requesting third-party payment platform account information about the user corresponding to the NFC token from an NFC token management platform; and the third-party payment platform performing payment processing according to the acquired third-party payment platform account information about the user, and sending payment information to the off-line charging party via the bank platform. The technical solution provided by the present invention enables an existing on-line payment system to support NFC-based mobile payment, which is not only favourable for the application and promotion of the NFC mobile payment mode in the field of payment, but also can prevent the waste of network equipment resources, and effectively enhances the flexibility of payment modes.

(57) 摘要:

[见续页]



WO 2017/012223 A1



本发明提供了基于 NFC 的移动支付方法和装置，其中的方法包括：第三方支付平台接收银行平台发送来的包含 NFC 令牌和订单信息的支付请求，其中，NFC 令牌由用户移动设备传输至线下收费方，且 NFC 令牌和订单信息经由线下收费方传输至银行平台；第三方支付平台向 NFC 令牌管理平台请求 NFC 令牌对应的用户的第三方支付平台账号信息；第三方支付平台根据获得的用户的第三方支付平台账号信息进行支付处理，并通过银行平台向线下收费方发送支付信息。本发明提供的技术方案使现有的线上支付系统支持基于 NFC 的移动支付，这不仅有利于 NFC 移动支付方式在支付领域中的使用推广，还可以避免网络设备资源的浪费，并有效增强了支付方式的灵活性。

基于 NFC 的移动支付方法和装置

相关申请的交叉引用

本申请请求于 2015 年 7 月 17 日提交的申请号为 201510425221.8 的中国专利申请的优先权，该中国专利申请的内容以引用方式被完整包含于此。

技术领域

本发明涉及网络技术，尤其是涉及一种基于 NFC 的移动支付方法以及基于 NFC 的移动支付装置。

背景技术

NFC (Near Field Communication, 近场通讯或近距离无线通讯) 是由非接触式 RFID (Radio Frequency Identification, 射频识别) 以及互联互通技术整合演变而来的一种短距离高频的无线电技术, 且 NFC 通常兼容 RFID。

目前, NFC 技术已经在一些国家得到了较为广泛的应用, 如 NFC 在移动支付尤其手机移动支付技术领域得到了较为广泛应用, 用户可以凭借其具有 NFC 功能 (即具有 NFC 模块) 的移动电话或者智能手表等用户移动设备实现移动支付。

在利用 NFC 来实现移动支付 (如手机移动支付) 的过程中, 通常并不需要移动电子设备接入网络, 移动电子设备通过使用 NFC 射频通道与 POS (point of sale, 销售点) 设备或者自动售货机等收费终端设备进行本地通讯, 由收费终端设备与网络侧进行信息交互, 以实现消费支付; 由此可知, NFC 移动支付实际上是一种线下支付方式。

发明人在实现本发明过程中发现, 目前的线下支付方式所涉及的线下支付体系和线上支付方式所涉及的线上支付体系是两套基本上相互独立的支付体系, 线上支付体系虽然随着网络的快速发展已经具有相当

的规模,但是线上支付体系并不支持 NFC 移动支付,两套体系的相互独立不仅使 NFC 移动支付方式在支付领域中的推广应用范围受到限制,而且,还会由于没有充分利用现有的两套支付体系而造成网络设备资源的浪费。

5

发明内容

本发明的目的是提供一种基于 NFC 的移动支付方法和装置。

根据本发明的其中一个方面,提供一种基于 NFC 的移动支付方法,且所述方法包括以下步骤:第三方支付平台接收银行平台发送来的包含近场通讯 NFC 令牌和订单信息的支付请求,其中,所述 NFC 令牌由用户移动设备基于 NFC 传输至线下收费方,并经由线下收费方将 NFC 令牌和订单信息传输至银行平台;第三方支付平台向 NFC 令牌管理平台请求所述 NFC 令牌对应的用户的第三方支付平台账号信息;第三方支付平台根据所述请求而获得的用户的第三方支付平台账号信息进行支付处理,并通过银行平台向线下收费方发送支付信息。

根据本发明的另一个方面,还提供一种基于 NFC 的移动支付装置,所述装置主要包括:第一接收模块,适于第三方支付平台接收银行平台发送来的包含近场通讯 NFC 令牌和订单信息的支付请求,其中,所述 NFC 令牌由用户移动设备基于 NFC 传输至线下收费方,并经由线下收费方将 NFC 令牌和订单信息传输至银行平台;请求处理模块,适于第三方支付平台向 NFC 令牌管理平台请求所述 NFC 令牌对应的用户的第三方支付平台账号信息;支付处理模块,适于第三方支付平台根据所述请求而获得的用户的第三方支付平台账号信息进行支付处理,并通过银行平台向线下收费方发送支付信息。

与现有技术相比,本发明具有以下优点:本发明通过使用户移动设备中的 NFC 令牌通过线下收费方以及银行平台传输至第三方支付平台,使用户在执行线下支付操作的情况下,针对线上支付的第三方支付平台可以获知该用户的基于线下的支付请求,从而使现有的线下支付体系和现有的线上支付体系能够互通;第三方支付平台通过向 NFC

令牌管理平台请求来获知该 NFC 令牌所对应的用户的第三方支付平台
账号信息，使第三方支付平台可以利用用户的线上账号对用户的线下
消费进行结算；由此可知，本发明提供的技术方案能够使现有的线上
支付系统和现有的线下支付系统结合起来，从而使现有的线上支付系
5 统可以支持基于 NFC 的移动支付，这不仅有利于基于 NFC 的移动支付
方式在支付领域中的使用推广，而且，还充分利用了现有的两套支付
系统，避免了网络设备资源的浪费，同时，本发明还有效增强了支付
方式的灵活性。

10 附图说明

通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，
本发明的其它特征、目的和优点将会变得更明显：

图 1 为本发明实施例一的基于 NFC 的移动支付方法流程图；

15 图 2 为本发明实施例二的百度虚拟银行卡空中发卡处理过程流程
图；

图 3 为本发明实施例二的用户刷卡进行支付的前端处理过程流程
图；

图 4 为本发明实施例二的用户刷卡进行支付的后端处理过程流程
图；

20 图 5 为本发明实施例三的基于 NFC 的移动支付方法流程图；

图 6 为本发明实施例四的基于 NFC 的移动支付方法流程图；

图 7 为本发明实施例五的基于 NFC 的移动支付装置示意图；

图 8 为本发明实施例六的基于 NFC 的移动支付装置示意图；

图 9 为本发明实施例七的基于 NFC 的移动支付装置示意图。

25 附图中相同或相似的附图标记代表相同或相似的部件。

具体实施方式

在更加详细地讨论示例性实施例之前应当提到的是，一些示例性实
施例被描述成作为流程图描绘的处理或者方法。虽然流程图将各项操作

描述成顺序的处理，但是，其中的许多操作可以被并行地、并发地或者同时实施。此外，各项操作的执行顺序可以被重新安排。当其操作执行完成时所述处理可以被终止，但是还可以具有未包括在附图中的附加步骤。所述处理可以对应于方法、函数、规程、子例程、子程序等等。

5 在上下文中所称的“平台”也可以称为“计算机设备”或“电脑”，是指可以通过运行预定程序或指令来执行数值计算和/或逻辑计算等预定处理过程的智能电子设备，其可以包括处理器以及存储器，由处理器执行在存储器中预存的存续指令来执行预定处理过程，或是由 ASIC、FPGA、DSP 等硬件执行预定处理过程，或是由上述二者组合来实现。计算机设
10 备包括但不限于服务器、个人电脑以及笔记本电脑等。

所述计算机设备包括用户设备与网络设备。其中，所述用户设备包括但不限于个人电脑以及笔记本电脑等；所述网络设备包括但不限于单个网络服务器、多个网络服务器组成的服务器组或者基于云计算（Cloud Computing）的由大量计算机或者网络服务器构成的云，其中，云计算
15 是分布式计算的一种，由一群松散耦合的计算机集组成的一个超级虚拟计算机。其中，所述计算机设备可单独运行来实现本发明，也可接入网络并通过与网络中的其他计算机设备的交互操作来实现本发明。其中，所述计算机设备所处的网络包括但不限于互联网、广域网、城域网、局域网、VPN 网络等。

20 需要说明的是，所述用户设备、网络设备以及网络等仅为举例，其他现有的或今后可能出现的计算机设备或网络如可适用于本发明，也应包含在本发明保护范围以内，并以引用方式包含于此。

下述文中所讨论的方法（其中一些通过流程图示出）可以通过硬件、软件、固件、中间件、微代码、硬件描述语言或者其任意组合来实施。
25 当用软件、固件、中间件或微代码来实施时，用以实施必要任务的程序代码或代码段可以被存储在机器或计算机可读介质（比如存储介质）中。（一个或多个）处理器可以实施必要的任务。

这里所公开的具体结构和功能细节仅仅是代表性的，并且是用于描述本发明的示例性实施例的目的。但是，本发明可以通过许多替换形式

来具体实现，并且不应当被解释成仅仅受限于这里所阐述的实施例。

应当理解的是，虽然在这里可能使用了术语“第一”、“第二”等等来描述各个单元，但是这些单元不应当受这些术语限制。使用这些术语仅仅是为了将一个单元与另一个单元进行区分。举例来说，在不背离示例性实施例的范围的情况下，第一单元可以被称为第二单元，并且类似地第二单元可以被称为第一单元。这里所使用的术语“和/或”包括其中一个或更多所列出的相关联项目的任意和所有组合。

应当理解的是，当一个单元被称为“连接”或者“耦合”到另一个单元时，其可以直接连接或者耦合到所述另一单元，或者可以存在中间单元。与此相对，当一个单元被称为“直接连接”或“直接耦合”到另一单元时，则不存在中间单元。应当按照类似的方式来解释被用于描述单元之间的关系的其他词语（例如“处于...之间”相比于“直接处于...之间”，“与...邻近”相比于“与...直接邻近”等等）。

这里所使用的术语仅仅是为了描述具体实施例而不意图限制示例性实施例。除非上下文明确地另有所指，否则这里所使用的单数形式“一个”、“一项”还意图包括复数。还应当理解的是，这里所使用的术语“包括”和/或“包含”规定所陈述的特征、整数、步骤、操作、单元和/或组件的存在，而不排除存在或添加一个或更多其他特征、整数、步骤、操作、单元、组件和/或其组合。

还应当提到的是，在一些替换实现方式中，所提到的功能/动作可按照不同于附图中标示的顺序发生。举例来说，取决于所涉及的功能/动作，相继示出的两幅图实际上可以基本上同时执行或有时可以按照相反的顺序来执行。

下面结合附图对本发明作进一步详细描述。

实施例一、基于 NFC 的移动支付方法。

图 1 为本实施例的基于 NFC 的移动支付方法的流程图，且图 1 所示的方法主要包括步骤 S100、步骤 S110 以及步骤 S120。本实施例所记载的方法可以在计算机设备中执行，如由第三方支付平台中的计算机设备执行。下面对图 1 中的各步骤分别进行说明。

S100、第三方支付平台接收银行平台发送来的包含有 NFC 令牌和订单信息的支付请求。

具体的，本实施例中的第三方支付平台接收到的 NFC 令牌(即 NFC token)是由用户移动设备通过 NFC 射频通道传输至线下收费方，并由线下收费方以及银行平台传输至第三方支付平台的。

作为示例，上述用户移动设备为具有 NFC 功能(即具有 NFC 模块)的用户移动设备，且该用户移动设备可以包括：智能移动电话、智能手表以及智能手环等可以安装 APP (Application, 应用) 或者 SDK (Software Development Kit, 软件开发工具包) 等应用软件的智能移动设备。本实施例不限制用户移动设备的具体表现形式。

作为示例，上述线下收费方可以包括线下收费终端设备以及收单方，其中的线下收费终端设备可以包括 POS 设备或者自动售货机等，而收单方可以为收单服务器等。在本示例中，第三方支付平台接收到的订单信息可以由线下收费终端设备产生，如线下收费终端设备根据用户本次消费产品以及商户编号等信息生成订单信息；线下收费终端设备产生的订单信息以及线下收费终端设备接收到的来自用户移动设备的 NFC 令牌在经由收单服务器以及银行平台后，被传输至第三方支付平台。

本实施例中的用户移动设备向线下收费终端设备传输的 NFC 令牌可以是经过加密处理的 NFC 令牌，也可以为未经过加密处理的 NFC 令牌；且线下收费方(如收费终端设备以及收单服务器)以及银行平台对其接收到的 NFC 令牌通常采用透传方式传输。

本实施例中的用户移动设备向线下收费方(如线下收费终端设备)发送的 NFC 令牌可以是用户在虚拟卡开卡申请过程中所获得的 NFC 令牌；也可以是用户在虚拟卡成功开卡之后，用户移动设备通过定期申请而获得的 NFC 令牌；还可以是用户移动设备在其内部设置的动态获取 NFC 令牌的功能被激活之后，用户移动设备从 NFC 令牌管理平台(如位于云端的 NFC 令牌管理服务器等)处动态申请而获得的 NFC 令牌。

本实施例所涉及的虚拟卡可以是针对第三方支付平台的，且具有发

卡行标识(bin)的卡,如虚拟卡的bin属于银联bin等,且通过该虚拟卡的bin可以确定出该虚拟卡是针对本实施例中的第三方支付平台的。第三方支付平台可以作为该虚拟卡的发卡行。该虚拟卡可以没有对应的真实存在的实物卡片,然而,该虚拟卡无论是在申请方面还是在管理
5 等环节都可以参考目前的银行卡(如银联卡)的相关环节。当然,本实施例也不排除该虚拟卡存在与之对应的真实存在的实物卡片的可能性。本实施例中的用户可以申请一张或者多张虚拟卡。

作为示例,用户移动设备在虚拟卡开卡申请过程中获取 NFC 令牌的一个具体例子为:用户打开用户移动设备中安装的相应 APP 或者
10 SDK 等(如点击用户移动设备显示界面中的 NFC 百度电子钱包 APP,进入 NFC 百度电子钱包 APP),并点击当前显示界面中的开卡按键,相应 APP 或者 SDK 会提示用户输入用户的第三方支付平台账号以及密码(如支付密码或者登录密码等),或者提示用户输入密码(用户的第三方支付平台账号可采用默认的账号或者前次输入的账号),在接收到
15 用户输入的账号和密码或者接收到用户输入的密码后,APP 或者 SDK 通过与第三方支付平台进行信息交互,以验证用户输入的密码是否正确,如果验证结果为用户输入了正确的密码,则 APP 或者 SDK 向第三方支付平台或者向 NFC 令牌管理平台发送虚拟卡开卡请求;如果第三方支付平台接收到来自用户的虚拟卡开卡请求,则第三方支付平台可以请求 NFC 令牌管理平台为该用户开设虚拟卡;NFC 令牌管理平台根据来自 APP/SDK 的请求或者来自第三方支付平台的请求执行为该用户
20 设置虚拟卡的操作,并利用预定算法对包括用户的第三方支付平台账号和虚拟卡发卡行识别码在内的信息进行计算,以便于为该用户生成 NFC 令牌,NFC 令牌管理平台可以对该 NFC 令牌进行加密处理,并将加密处理后的 NFC 令牌下发给用户移动设备;NFC 令牌管理平台也可以不对 NFC 令牌进行加密处理,而是直接将其计算生成的 NFC 令牌下发给用户移动设备。NFC 令牌可以由 NFC 令牌管理平台直接下发给用户移动设备,也可以由 NFC 令牌管理平台通过第三方支付平台下发给用户移动设备;用户移动设备在接收到 NFC 令牌后,可以将该 NFC 令
25

牌本地安全存储，如 NFC 令牌可以存储于智能 Sdcard (Secure Digital Memory Card, 安全数字存储卡) 或者 SIM (Subscriber Identity Module, 客户识别模块) 卡中，也可以存储于 TrustZone (可信区) 或者 TPM (Trusted Platform Module, 可信赖平台模块) 中。该 NFC 令牌可以多次有效使用，也可以单次有效使用或者根据限制性条款而有效使用。

在申请了虚拟卡之后，用户可以针对 NFC 支付设置对应的支付银行卡以及支付方式等支付规则信息，例如，设置是否优先使用用户的百度钱包账户中的余额进行支付的规则，再例如，设置在用户的百度钱包账户中的余额不足时，优先选择用于支付的银行卡的规则等。用户设置的支付规则信息可以存储于第三方支付平台和/或 NFC 令牌管理平台中。本实施例不限制用户针对 NFC 支付所设置的支付规则信息包含的内容以及存储方式。

作为示例，用户移动设备在已经成功申请了虚拟卡之后，动态获取 NFC 令牌的一个具体例子为：用户打开用户移动设备中安装的相应 APP (如 NFC 百度电子钱包 APP) 或者 SDK 等，并点击显示界面中的登录按键，相应 APP 或者 SDK 会提示用户输入用户的第三方支付平台账号以及密码，或者提示用户输入密码 (用户的第三方支付平台账号可采用默认的账号或者前次输入的账号)，在接收到用户输入的账号以及密码或者接收到密码后，相应 APP 或者 SDK 通过与第三方支付平台进行信息交互来验证用户输入的密码是否正确，如果验证结果为用户输入了正确的密码，则相应 APP 或者 SDK 向第三方支付平台或者向 NFC 令牌管理平台发送 NFC 令牌请求，且第三方支付平台在接收到来自用户的 NFC 令牌请求后，可以请求 NFC 令牌管理平台为该用户下发 NFC 令牌，NFC 令牌管理平台根据来自 APP/SDK 的请求或者来自第三方支付平台的请求利用预定算法对包括用户的第三方支付平台账号以及虚拟卡发卡行识别码在内的信息进行计算，以便于为该用户生成 NFC 令牌，NFC 令牌管理平台可以对该 NFC 令牌进行加密处理，并将加密处理后的 NFC 令牌下发给用户移动设备；NFC 令牌管理平台也可以不对该 NFC 令牌进行加密处理，而是直接将其计算生成的 NFC 令牌下发给

用户移动设备。NFC 令牌可以由 NFC 令牌管理平台直接下发给用户移动设备，也可以由 NFC 令牌管理平台通过第三方支付平台下发给用户移动设备；用户移动设备在接收到 NFC 令牌后，可以将该 NFC 令牌存储于本地安全区域中，如存储于 NFC SE 模块中等。

- 5 作为示例，NFC 令牌管理平台生成的 NFC 令牌可以存在使用限制，如 NFC 令牌具有时效性和/或地域有效性和/或使用次数有效性。这里的时效性是指 NFC 令牌在某段时间范围内有效，如果来自用户移动设备的 NFC 令牌已经超出了其对应的有效时间范围，则该 NFC 令牌不能应用于本次支付过程中，用户移动设备可以重新申请 NFC 令牌；这
- 10 里的地域有效性是指 NFC 令牌在某地域范围内有效，NFC 令牌管理平台可以在用户每次使用相应 APP (Application, 应用) 或者 SDK 时获取用户移动设备的位置信息，并将最近一次获取到的位置信息作为 NFC 令牌当前所处的位置，如果 NFC 令牌当前所处的位置不属于指定的位置区域（如用户在虚拟卡开卡过程中设定的位置区域或者在后续的虚拟
- 15 卡使用过程中设定的位置区域），则该 NFC 令牌不能应用于本次支付过程中，用户移动设备可以重新申请 NFC 令牌；这里的使用次数有效性是指一个 NFC 令牌可以被用户使用的次数，如果 NFC 令牌当前使用次数已经达到了预定次数（如用户在虚拟卡开卡过程中设定的预定次数或者在后续的虚拟卡使用过程中设定的预定次数或者 NFC 令牌管理平台
- 20 为 NFC 令牌设置的缺省使用次数等），则该 NFC 令牌不能应用于本次支付过程中，用户移动设备可以重新申请 NFC 令牌。

- 25 作为示例，第三方支付平台接收银行平台发送来的支付请求的一个具体过程为：线下收费终端设备根据用户的消费产生相应的订单信息，该订单信息可以包括订单号以及本次消费金额等信息，线下收费终端设备扫描用户移动设备，以请求用户移动设备通过 NFC 射频通道向其传输 NFC 令牌，用户移动设备在向线下收费终端设备传输 NFC 令牌之前，可以对用户身份进行验证（如利用指纹或者声音或者面孔或者密码等方式实现用户身份的验证），在用户身份验证成功的情况下，用户移动设备通过 NFC 射频通道向线下收费终端设备传输其存储的 NFC

令牌，否则，用户移动设备拒绝向线下收费终端设备传输 NFC 令牌，且用户移动设备可以通过 NFC 射频通道向线下收费终端设备返回拒绝传输 NFC 令牌的原因；线下收费终端设备在通过 NFC 射频通道成功接收到 NFC 令牌后，将其产生的订单信息以及接收到的 NFC 令牌一起传输给与其连接的收单方（也可以称为收单平台，如收单服务器等），并由收单方将 NFC 令牌和订单信息一起通过互联网传输给银行平台（如银行服务器或者银联服务器等）；针对 NFC 令牌而言，线下收费终端设备以及收单方均可以采用透传方式进行传输；银行平台在接收到 NFC 令牌以及订单信息后，可以根据 NFC 令牌获得虚拟卡发卡行标识，由于虚拟卡发卡行识别码表征第三方支付平台，因此，银行平台可以根据该虚拟卡发卡行标识判断出其接收到的订单信息需要由第三方支付平台支付，从而银行平台将 NFC 令牌以及订单信息通过支付请求发送给第三方支付平台。

在上述示例中，用户移动设备完全可以在自身内部实现对用户身份的验证，例如用户移动设备在接收到 NFC 令牌请求后，提示用户执行指纹采集操作，用户移动设备对采集到的指纹进行指纹特征提取处理，并将提取出的指纹特征与其内部存储的指纹特征进行比对，用户移动设备根据指纹特征比对结果确定本次用户身份验证是否通过；再例如，用户移动设备在接收到 NFC 令牌请求后，提示用户执行刷脸操作，用户移动设备对刷脸获得的面部图像进行面部特征提取处理，并将提取出的面部特征与其内部存储的面部特征进行比对，用户移动设备根据面部特征比对结果确定本次用户身份验证是否通过；再例如，用户移动设备在接收到 NFC 令牌请求后，提示用户执行声音采集操作，用户移动设备对采集到的声音进行音频特征提取处理，并将提取出的音频特征与其内部存储的音频特征进行比对，用户移动设备根据音频特征比对结果确定本次用户身份验证是否通过；再例如，用户移动设备在接收到 NFC 令牌请求后，提示用户输入身份验证密码，将用户输入的身份验证密码与其内部存储的密码进行匹配，用户移动设备根据密码匹配结果确定本次用户身份验证是否通过。

在上述示例中，用户移动设备也可以借助网络中的相应设备来实现对用户身份的验证，例如，上述示例中的指纹特征提取和比对过程、面部特征提取和比对过程、音频特征提取和比对过程以及密码匹配过程可以由网络侧中的相应设备（如第三方支付平台或者网络中的身份验证服务器等）来执行。在由网络侧中的相应设备来执行用户身份验证的情况下，通常需求用户移动设备能够接入网络。

在上述示例中，银行平台根据接收到的 NFC 令牌获得虚拟卡发卡行标识的过程可以具体为：银行平台在接收到收单服务器传输来的 NFC 令牌和订单信息后，通过调用 NFC 令牌管理平台提供的接口来获得 NFC 令牌对应的虚拟卡发卡行标识，即银行平台通过调用 NFC 令牌管理平台提供的接口将 NFC 令牌传输给 NFC 令牌管理平台，以请求获得虚拟卡发卡行标识，如果 NFC 令牌为加密后的 NFC 令牌，则 NFC 令牌管理平台先利用其存储的解密密钥对该 NFC 令牌进行解密处理，然后，NFC 令牌管理平台利用预先设置的预定算法对解密处理后的 NFC 令牌进行计算处理，并从计算处理结果中提取出虚拟卡发卡行标识，NFC 令牌管理平台将该提取出的虚拟卡发卡行标识返回给银行平台；如果 NFC 令牌为未进行加密的 NFC 令牌，则 NFC 令牌管理平台可以直接利用其预先设置的预定算法对该 NFC 令牌进行处理，并从处理结果中提取出虚拟卡发卡行标识，NFC 令牌管理平台将该虚拟卡发卡行标识返回给银行平台。

在上述示例中，银行平台根据接收到的 NFC 令牌获得虚拟卡发卡行标识的过程也可以具体为：银行平台在接收到收单服务器传输来的 NFC 令牌和订单信息后，通过调用 NFC 令牌管理平台提供的接口来获得 NFC 令牌对应的用户的第三方支付平台账号以及虚拟卡发卡行标识等信息，即银行平台通过调用 NFC 令牌管理平台提供的接口将 NFC 令牌传输给 NFC 令牌管理平台，以请求获得虚拟卡发卡行标识，如果 NFC 令牌为加密后的 NFC 令牌，则 NFC 令牌管理平台先利用其存储的解密密钥对该 NFC 令牌进行解密处理，然后，NFC 令牌管理平台利用预先设定的预定算法对解密处理后的 NFC 令牌进行计算处理，并将计算处

理结果返回给银行平台；如果 NFC 令牌为未进行加密的 NFC 令牌，则 NFC 令牌管理平台可以直接利用其预先设定的预定算法对该 NFC 令牌进行计算处理，并将计算处理结果返回给银行平台。银行平台从 NFC 令牌管理平台返回的包含有用户的第三支付平台账号以及虚拟卡发卡行标识的信息中获取虚拟卡发卡行标识。

在上述示例中，银行平台根据接收到的 NFC 令牌获得虚拟卡发卡行标识的过程也可以具体为：银行平台在接收到收单服务器传输来的 NFC 令牌以及订单信息后，先通过调用 NFC 令牌管理平台提供的接口来获得 NFC 令牌对应的解密密钥以及预定算法，即银行平台通过调用 NFC 令牌管理平台提供的接口将其接收到的 NFC 令牌传输给 NFC 令牌管理平台，以请求获得虚拟卡发卡行标识，NFC 令牌管理平台将其存储的该 NFC 令牌对应的解密密钥以及预先设定的预定算法返回给银行平台；之后，银行平台利用接收到的解密密钥对 NFC 令牌进行解密处理，并利用接收到的预定算法对解密处理后的 NFC 令牌进行计算处理，银行平台从计算处理结果中提取出虚拟卡发卡行标识。

在上述示例中，银行平台根据接收到的 NFC 令牌获得虚拟卡发卡行标识的过程还可以具体为：银行平台在接收到收单服务器传输来的 NFC 令牌以及订单信息后，先通过调用 NFC 令牌管理平台提供的接口来获得解密后的 NFC 令牌，即银行平台通过调用 NFC 令牌管理平台提供的接口将其接收到的 NFC 令牌传输给 NFC 令牌管理平台，以请求获得虚拟卡发卡行标识，NFC 令牌管理平台利用其存储的解密密钥对该 NFC 令牌进行解密处理，并将解密处理后的 NFC 令牌返回给银行平台；之后，银行平台利用其存储的预定算法对解密后的 NFC 令牌进行计算处理，并从计算处理结果中提取出虚拟卡发卡行标识。

需要说明的是，在银行平台需要利用其存储的预定算法对 NFC 令牌进行计算处理的情况下，银行平台通常是通过与 NFC 令牌管理平台之间的信息交互预先获得并存储 NFC 令牌对应的预定算法，例如，银行平台通过与 NFC 令牌管理平台之间进行信息交互获得 NFC 令牌管理平台中的默认预定算法并本地存储，银行平台可以利用其存储的该默

认预定算法对多个 NFC 令牌分别进行计算，以从计算结果中获取虚拟卡发卡行标识，这样，银行平台可以不需要在每次接收到 NFC 令牌以及订单信息时均需要向 NFC 令牌管理平台请求预定算法。

本实施例不限制银行平台获得 NFC 令牌对应的解密密钥以及预定
5 算法的具体实现方式，也不限制银行平台获得虚拟卡发卡行标识以及银行平台向第三方支付平台发送支付请求的具体实现过程。

S110、第三方支付平台向 NFC 令牌管理平台请求 NFC 令牌对应的用户的第三方支付平台账号信息。

具体的，第三方支付平台可以利用 NFC 令牌管理平台提供的接口
10 向 NFC 令牌管理平台请求 NFC 令牌对应的用户的第三方支付平台账号信息；一个具体的例子为：第三方支付平台通过调用 NFC 令牌管理平台提供的接口将 NFC 令牌传输给 NFC 令牌管理平台，如果 NFC 令牌为加密后的 NFC 令牌，则 NFC 令牌管理平台应先对该 NFC 令牌进行解密处理，然后，NFC 令牌管理平台利用预定算法对解密后的 NFC 令牌进
15 行计算处理，并从计算处理结果中提取出用户的第三方支付平台账号信息，NFC 令牌管理平台将该用户的第三方支付平台账号信息返回给第三方支付平台；如果 NFC 令牌为未进行加密的 NFC 令牌，则 NFC 令牌管理平台直接利用预定算法对该 NFC 令牌进行计算处理，并从计算处理结果中提取出用户的第三方支付平台账号信息，NFC 令牌管理平台将该用户的第三方支付平台账号信息返回给第三方支付平台。另一个具体的例子为：第三方支付平台通过调用 NFC 令牌管理平台提供的接口将 NFC 令牌传输给 NFC 令牌管理平台，在 NFC 令牌为加密后的 NFC 令牌的情况下，NFC 令牌管理平台将该 NFC 令牌的解密密钥返回
20 给第三方支付平台，第三方支付平台利用该解密密钥对 NFC 令牌进行解密处理，然后，NFC 令牌管理平台利用预定算法对解密后的 NFC 令牌进行计算处理，并从计算处理结果中提取出用户的第三方支付平台账号信息；在该例子中，第三方支付平台可以通过与 NFC 令牌管理平台之间的信息交互获得 NFC 令牌对应的预定算法，如第三方支付平台通过与 NFC 令牌管理平台之间进行信息交互获得 NFC 令牌管理平台中
25

的默认预定算法，第三方支付平台可以利用该默认预定算法对多个 NFC 令牌分别进行计算，以从计算结果中获取用户的第三方支付平台账号信息。

作为示例，第三方支付平台可以先对其接收到的支付请求进行验证（如验证该支付请求是否为有效的支付请求等），并在验证通过的情况下，第三方支付平台向 NFC 令牌管理平台请求该 NFC 令牌对应的用户的第三方支付平台账号信息。

作为示例，在 NFC 令牌管理平台生成的 NFC 令牌存在使用限制（如 NFC 令牌具有时效性和/或地域有效性和/或使用次数有效性）的情况下，NFC 令牌管理平台可以对来自第三方支付平台的 NFC 令牌进行有效性验证，并在本次有效性验证通过的情况下，向第三方支付平台返回该 NFC 令牌对应的相关信息；如在该 NFC 令牌仍然处于某段时间范围内和/或者在该 NFC 令牌仍然属于某地域范围内和/或者该 NFC 令牌已经被用户使用的次数仍然没有达到预定次数等情况下，确定本次有效性验证通过；否则本次有效性验证失败。在有效性验证失败的情况下，NFC 令牌管理平台可以向第三方支付平台返回有效性验证失败的信息，且 NFC 令牌管理平台还可以要求用户移动设备重新申请 NFC 令牌，如 NFC 令牌管理平台通过第三方支付平台、银行平台以及线下收费方向用户移动终端下发要求其重新申请 NFC 令牌的信息。

NFC 令牌管理平台中存储有 NFC 令牌和用户的第三方支付平台账号信息这两者之间的对应关系信息，进一步的，NFC 令牌管理平台中存储有 NFC 令牌、用户的第三方支付平台账号信息以及虚拟卡发卡行标识这三者之间的对应关系信息，NFC 令牌管理平台可以根据接收到的 NFC 令牌查找到与之对应的用户的第三方支付平台账号信息或者虚拟卡发卡行标识。NFC 令牌管理平台可以利用表或者数据库等方式存储上述对应关系，且上述对应关系可以由 NFC 令牌管理平台进行动态维护，如增加新的对应关系或者删除相应的对应关系或者标记某个 NFC 令牌已失效或者针对某个对应关系产生新的 NFC 令牌并利用该新的 NFC 令牌替换旧的 NFC 令牌等。本实施例不限制 NFC 令牌管理平台

存储对应关系的具体实现方式以及动态维护对应关系的具体实现方式。

S120、第三方支付平台根据上述请求而获得的用户的第三方支付平台账号信息进行支付处理，并通过银行平台向线下收费方发送支付信息。

具体的，第三方支付平台在基于请求而获得了用户的第三方支付平台账号信息之后，可以向用户权益管理平台（如用户权益管理服务器）请求该用户的用户权益信息，如第三方支付平台通过调用用户权益管理平台提供的接口将该用户的第三方支付平台账号信息传输给用户权益管理平台，并接收用户权益管理平台返回的用户权益信息（如优惠券和/或积分等）。第三方支付平台可以在获得了用户权益管理平台返回的用户权益信息的基础上进行支付处理，如根据用户权益信息计算用户针对本次订单而需要支付的金额（即当前支付金额）等。本实施例中的第三方支付平台通过在支付处理过程中引入用户权益信息，在很大程度上提高了线下支付结算的灵活性。

另外，第三方支付平台还可以将其接收到的订单信息提供给用户权益管理平台，如在支付处理之前或者在支付处理成功完成之后，第三方支付平台将订单信息提供给用户权益管理平台，以便于使用户权益管理平台可以针对用户的本次消费及时的更新用户当前的用户权益信息。本实施例中的第三方支付平台通过将订单信息提供给用户权益管理平台，这样，本实施例不仅可以在本次支付过程中使用用户权益，还可以使本次消费贡献于用户权益，从而形成支付以及用户权益的闭环。

第三方支付平台可以根据用户预先为 NFC 支付设置的支付银行卡以及支付方式等信息按照现有的线上支付流程执行相应的操作，如第三方支付平台采用快捷支付方式进行支付扣款等。

第三方支付平台可以通过银行平台向线下收费方发送支付信息，以便于收费方完成本次费用收取。银行平台可以采用透传方式向线下收费方传输该支付信息。本实施例中的支付信息除了包括当前支付金额

之外，还可以包括订单号、本次使用的用户积分信息以及优惠信息等。本实施例不限制第三方支付平台向收费方下发的支付信息所包含的具体内容。

由上述描述可知，本实施例可以通过与用户移动设备进行一次信息交互（即传输 NFC 令牌的交互）即可完成费用支付以及用户权益核销等过程，使线下支付具有较好的便捷性。

实施例二、基于 NFC 的移动支付方法。

下面以 NFC 百度电子钱包为例对本实施例的方法进行详细说明。本实施例方法主要包括百度虚拟银行卡（即虚拟卡）空中发卡处理过程、用户刷卡进行支付的前端处理过程及用户刷卡进行支付的后端处理过程三部分内容。

百度虚拟银行卡空中发卡处理过程的流程如图 2 所示。

图 2 中，S20、用户打开其移动电话中的 NFC 百度电子钱包 APP。

S21、NFC 百度电子钱包 APP 提示用户输入百度钱包账号信息以及支付密码，即 NFC 百度电子钱包的用户应该为百度钱包的用户。

S22、NFC 百度电子钱包 APP 接收用户输入的百度钱包账号信息以及支付密码。

S23、NFC 百度电子钱包 APP 通过与百度钱包支付服务器（即第三方支付平台）进行信息交互来验证用户输入的百度钱包账号信息以及支付密码是否正确。

S24、在验证结果为用户输入的百度钱包账号信息以及支付密码均正确的情况下，NFC 百度电子钱包 APP 根据用户点击的开卡按钮的操作向 NFC Token 管理服务器发送百度虚拟银行卡开卡申请（即虚拟卡开卡申请）。

S25、NFC Token 管理服务器根据接收到的虚拟卡开卡申请为用户生成虚拟卡卡号，该虚拟卡卡号可以包括用户的百度钱包账号和百度虚拟银行 bin。

S26、NFC Token 管理服务器根据预定算法对用户的虚拟卡卡号进行计算处理，从而为用户生成 NFC Token。

S27、NFC Token 管理服务器对上述 NFC Token 进行加密处理，获得加密处理后的 NFC Token。

S28、NFC Token 管理服务器向 NFC 百度电子钱包 APP 下发加密处理后的 NFC Token。

5 S29、NFC 百度电子钱包 APP 将接收到的 NFC Token 存储于本地安全区域，并提示用户虚拟卡开卡成功完成。

本实施例在步骤 S24 中或者在步骤 S29 之后，可以为 NFC 支付设置对应的支付银行卡以及支付方式（如是否优先使用用户的百度钱包账户中的余额进行支付等），用户的设置信息应存储于第三方支付平台中。

10 用户刷卡进行支付的前端处理过程的流程如图 3 所示。

图 3 中，S30、用户将其移动电话靠近 POS 设备，以进行无接触刷卡。

S31、POS 设备向用户移动电话返回应用选择信息，以使用户选择本次是否利用其 NFC 百度电子钱包进行本次消费支付。

15 S32、在用户确认利用其 NFC 百度电子钱包来支付本次消费的情况下，NFC 百度电子钱包 APP 提示用户进行身份验证，如提示用户执行指纹输入操作或者声音输入操作或者刷脸操作等。

S33、NFC 百度电子钱包 APP 接收用户输入的指纹或者声音或者面部图像或者身份验证密码等信息。

20 S34、NFC 百度电子钱包 APP 根据接收到的信息对用户进行身份验证，如 NFC 百度电子钱包 APP 通过与百度钱包支付服务器（即第三方支付服务器）进行信息交互以对用户进行身份验证或者在本地对用户进行身份验证等。

25 S35、在用户身份验证通过的情况下，NFC 百度电子钱包 APP 与 POS 设备建立安全通信通道，并从本地安全区域读取加密后的 NFC Token。

S36、NFC 百度电子钱包 APP 通过安全通信通道将读取的 NFC Token 传输给 POS 设备。

S37、POS 设备在接收到 NFC Token 之后，执行后续支付处理操

作，如将 NFC Token 和其生成的订单信息传输给收单服务器，并等待收单服务器返回的信息等。

S38、POS 设备在根据接收到的收单服务器返回的信息确定本次支付成功完成时，提示用户本次支付成功完成。

5 用户刷卡进行支付的后端处理过程的流程如图 4 所示。

图 4 中，S40、在用户将其移动电话靠近 POS 设备时，POS 设备与移动电话之间进行无接触刷卡，POS 设备接收到用户移动电话传输来的加密后的 NFC Token。

S41、POS 设备将加密后的 NFC Token 传输至收单方。

10 S42、收单方通过银联服务器向百度钱包支付服务器发送包含有加密后的 NFC Token 以及订单信息的支付请求。

S43、百度钱包支付服务器在接收到支付请求后，执行 NFC Token 解密以及有效性验证操作，如通过调用 NFC Token 管理服务器提供的接口，使 NFC Token 管理服务器对 NFC Token 进行解密以及有效性验证，并向百度钱包支付服务器返回用户的百度钱包账号信息。

S44、百度钱包支付服务器获取用户权益信息，并根据用户权益信息计算用户本次消费的实际支付金额。

S45、百度钱包支付服务器根据用户预先为 NFC 支付设置的支付银行卡按照现有的线上支付流程执行相应的操作，如请求支付银行卡对应的支付方进行支付扣款等

S46、百度钱包支付服务器向银联服务器返回支付完成信息，银联服务器向收单方返回支付完成信息。

S47、收单方向 POS 设备返回支付完成信息，本次支付过程结束。

实施例三、基于 NFC 的移动支付方法。

25 图 5 为本实施例的基于 NFC 的移动支付方法的流程图，且图 5 所示的方法主要包括步骤 S500 以及步骤 S510。本实施例所记载的方法可以在计算机设备中执行，如在银行平台中的相应计算机设备中执行。下面对图 5 中的各步骤分别进行说明。

S500、银行平台接收线下收费方发送来的包含 NFC 令牌和订单信

息的支付请求。

具体的，银行平台接收到的 NFC 令牌是由用户移动设备基于 NFC 传输至线下收费方，并由线下收费方将其产生的订单信息与该 NFC 令牌一起发送给银行平台的。另外，银行平台接收到的 NFC 令牌可以是
5 经过加密处理的 NFC 令牌，也可以为未经过加密处理的 NFC 令牌；且银行平台对其接收到的 NFC 令牌通常采用透传方式传输。

S510、在银行平台根据其接收到的 NFC 令牌获取到虚拟卡发卡行标识的情况下，银行平台根据虚拟卡发卡行标识向第三方支付平台发送该支付请求。

10 作为示例，银行平台根据接收到的 NFC 令牌获得相应的虚拟卡发卡行标识的过程可以为：银行平台在接收到收单服务器传输来的 NFC 令牌和订单信息后，通过调用 NFC 令牌管理平台提供的接口来获得 NFC 令牌对应的虚拟卡发卡行标识，即银行平台通过调用 NFC 令牌管理平台提供的接口将 NFC 令牌传输给 NFC 令牌管理平台，以请求获得
15 虚拟卡发卡行标识，如果 NFC 令牌为加密后的 NFC 令牌，则 NFC 令牌管理平台先利用其存储的解密密钥对该 NFC 令牌进行解密处理，然后，NFC 令牌管理平台利用预先设置的预定算法对解密处理后的 NFC 令牌进行计算处理，并从计算处理结果中提取出虚拟卡发卡行标识，NFC 令牌管理平台将该提取出的虚拟卡发卡行标识返回给银行平台；
20 如果 NFC 令牌为未进行加密的 NFC 令牌，则 NFC 令牌管理平台可以直接利用其预先设置的预定算法对该 NFC 令牌进行处理，并从处理结果中提取出虚拟卡发卡行标识，NFC 令牌管理平台将该虚拟卡发卡行标识返回给银行平台。

25 作为示例，银行平台根据接收到的 NFC 令牌获得相应的虚拟卡发卡行标识的过程可以为：银行平台在接收到收单服务器传输来的 NFC 令牌和订单信息后，通过调用 NFC 令牌管理平台提供的接口来获得 NFC 令牌对应的用户的第三支付平台账号以及虚拟卡发卡行标识等信息，即银行平台通过调用 NFC 令牌管理平台提供的接口将 NFC 令牌传输给 NFC 令牌管理平台，以请求获得虚拟卡发卡行标识，如果 NFC 令

牌为加密后的 NFC 令牌，则 NFC 令牌管理平台先利用其存储的解密密钥对该 NFC 令牌进行解密处理，然后 NFC 令牌管理平台利用预先设定的预定算法对解密处理后的 NFC 令牌进行计算处理，并将计算处理结果返回给银行平台；如果 NFC 令牌为未进行加密的 NFC 令牌，则 NFC 令牌管理平台可以直接利用其预先设定的预定算法对该 NFC 令牌进行计算处理，并将计算处理结果返回给银行平台。银行平台从 NFC 令牌管理平台返回的包含有用户的第三支付平台账号以及虚拟卡发卡行标识的信息中获取虚拟卡发卡行标识。

作为示例，银行平台根据接收到的 NFC 令牌获得相应的虚拟卡发卡行标识的过程可以为：银行平台在接收到收单服务器传输来的 NFC 令牌以及订单信息后，先通过调用 NFC 令牌管理平台提供的接口来获得 NFC 令牌对应的解密密钥以及预定算法，即银行平台通过调用 NFC 令牌管理平台提供的接口将其接收到的 NFC 令牌传输给 NFC 令牌管理平台，以请求获得虚拟卡发卡行标识，NFC 令牌管理平台将其存储的该 NFC 令牌对应的解密密钥以及预先设定的预定算法返回给银行平台；之后，银行平台利用接收到的解密密钥对 NFC 令牌进行解密处理，并利用接收到的预定算法对解密处理后的 NFC 令牌进行计算处理，银行平台从计算处理结果中提取出虚拟卡发卡行标识。

作为示例，银行平台根据接收到的 NFC 令牌获得相应的虚拟卡发卡行标识的过程可以为：银行平台在接收到收单服务器传输来的 NFC 令牌和订单信息后，通过调用 NFC 令牌管理平台提供的接口来获得解密后的 NFC 令牌，即银行平台通过调用 NFC 令牌管理平台提供的接口将其接收到的 NFC 令牌传输给 NFC 令牌管理平台，以请求获得虚拟卡发卡行标识，NFC 令牌管理平台利用其存储的解密密钥对该 NFC 令牌进行解密处理，并将解密处理后的 NFC 令牌返回给银行平台；之后，银行平台利用其存储的预定算法对解密后的 NFC 令牌进行计算处理，并从计算处理结果中提取出虚拟卡发卡行标识。

需要说明的是，在银行平台需要利用其存储的预定算法对 NFC 令牌进行计算处理的情况下，银行平台通常是通过与 NFC 令牌管理平台

之间的信息交互预先获得并存储 NFC 令牌对应的预定算法, 例如, 银行平台通过与 NFC 令牌管理平台之间进行信息交互获得 NFC 令牌管理平台中的默认预定算法并本地存储, 银行平台可以利用其存储的该默认预定算法对多个 NFC 令牌分别进行计算, 以从计算结果中获取虚拟卡发卡行标识, 这样, 银行平台可以不需要在每次接收到 NFC 令牌以及订单信息时均需要向 NFC 令牌管理平台请求预定算法。

本实施例不限制银行平台获得 NFC 令牌对应的解密密钥以及预定算法的具体实现方式, 也不限制银行平台获得虚拟卡发卡行标识以及银行平台向第三方支付平台发送支付请求的具体实现过程。

实施例四、基于 NFC 的移动支付方法。

图 6 为本实施例的基于 NFC 的移动支付方法的流程图, 且图 6 所示的方法主要包括步骤 S600、步骤 S610 以及步骤 S620。本实施例所记载的方法可以在计算机设备中执行, 如该方法在 NFC 令牌管理平台中的相应计算机设备中执行。下面对图 6 中的各步骤分别进行说明。

S600、NFC 令牌管理平台接收用户的虚拟卡开卡申请。

具体的, NFC 令牌管理平台接收到的虚拟卡开卡申请可以是用户移动设备直接传输来的, 也可以是用户移动设备向第三方支付平台进行虚拟卡开卡申请, 且第三方支付平台根据用户移动设备的申请而向 NFC 令牌管理平台传输的虚拟卡开卡申请。

S610、NFC 令牌管理平台为虚拟卡开卡申请设置虚拟卡发卡行标识。

具体的, 虚拟卡发卡行识别码用于表征第三方支付平台, 即虚拟卡是针对第三方支付平台, 且具有发卡行标识 (bin) 的卡, 如虚拟卡的 bin 属于银联 bin 等, 通过该虚拟卡的 bin 可以确定出该虚拟卡是针对第三方支付平台的; 也就是说, 第三方支付平台可以作为该虚拟卡的发卡行。该虚拟卡可以没有对应的真实存在的实物卡片, 然而, NFC 令牌管理平台可以参考目前的银行卡 (如银联卡) 的相关环节对虚拟卡的申请以及管理等环节进行维护管理。当然, 本实施例也不排除该虚拟卡存在与之对应的真实存在的实物卡片的可能性。本实施例中的用户

可以申请一张或者多张虚拟卡。

S620、NFC 令牌管理平台根据用户的第三方支付平台账号信息和虚拟卡发卡行标识生成 NFC 令牌，并将该 NFC 令牌下发给用户移动设备。

5 具体的，NFC 令牌管理平台可以利用预定算法对包括用户的第三方支付平台账号和虚拟卡发卡行识别码在内的信息进行计算，从而为该用户生成 NFC 令牌，NFC 令牌管理平台可以对该 NFC 令牌进行加密处理，并将加密处理后的 NFC 令牌下发给用户移动设备；NFC 令牌管理平台也可以不对 NFC 令牌进行加密处理，而是直接将其计算生成的
10 NFC 令牌下发给用户移动设备。NFC 令牌管理平台可以将 NFC 令牌直接下发给用户移动设备，也可以通过第三方支付平台将 NFC 令牌下发给用户移动设备。

 NFC 令牌管理平台生成的 NFC 令牌可以存在使用限制，如 NFC 令牌具有时效性和/或地域有效性和/或使用次数有效性等，具体请参见上
15 述实施例一中的描述。

 NFC 令牌管理平台可以根据银行平台以及第三方支付平台的请求而向银行平台以及第三方支付平台返回与 NFC 令牌相关的信息，如 NFC 令牌管理平台根据来自银行平台的 NFC 令牌向银行平台返回虚拟卡发卡行标识；再如 NFC 令牌管理平台根据来自第三方支付平台的 NFC 令牌向第三方支付平台返回用户的第三方支付账号信息等。另外，NFC
20 令牌管理平台在根据银行平台以及第三方支付平台的请求而向银行平台以及第三方支付平台返回与 NFC 令牌相关的信息的过程中，可以根据 NFC 令牌的使用限制对接收到的 NFC 令牌进行有效性验证，在有效性验证通过的情况下，NFC 令牌管理平台向银行平台以及第三方支付
25 平台返回与 NFC 令牌相关的信息，而在有效性验证失败的情况下，NFC 令牌管理平台可以要求用户重新申请 NFC 令牌。

 NFC 令牌管理平台不仅可以在用户申请虚拟卡的过程中，为用户生成 NFC 令牌，还可以在用户具有虚拟卡之后，根据用户的申请而为用户动态生成 NFC 令牌。具体请参见上述实施例一中的描述，在此不再

详细说明。

实施例五、基于 NFC 的移动支付装置。

本实施例的装置可以设置于计算机设备中，且该装置可以形成第三方支付平台，该装置的主要结构如图 7 所示。

5 图 7 中，基于 NFC 的移动支付装置主要包括：第一接收模块 700、请求处理模块 710 以及支付处理模块 720。

第一接收模块 700 主要适于第三方支付平台接收银行平台发送来的包含近场通讯 NFC 令牌和订单信息的支付请求。

10 具体的，第一接收模块 700 接收到的 NFC 令牌是由用户移动设备通过 NFC 射频通道传输至线下收费方，并经由线下收费方以及银行平台传输至第三方支付平台的，第一接收模块 700 接收到的订单信息是由线下收费方产生，并经由银行平台传输至第三方支付平台的；且第一接收模块 700 接收到的 NFC 令牌可以是经过加密处理的 NFC 令牌，也可以为未经过加密处理的 NFC 令牌。

15 第一接收模块 700 接收到的 NFC 令牌可以是用户在虚拟卡开卡申请过程中所获得的 NFC 令牌，也可以是用户在虚拟卡成功开卡之后，用户移动设备通过定期申请或者其内部设置的动态获取 NFC 令牌的功能被激活之后，用户移动设备从 NFC 令牌管理平台（如位于云端的 NFC 令牌管理服务器等）处动态申请而获得的 NFC 令牌。

20 请求处理模块 710 主要适于第三方支付平台向 NFC 令牌管理平台请求 NFC 令牌对应的用户的第三方支付平台账号信息。

25 具体的，请求处理模块 710 可以利用 NFC 令牌管理平台提供的接口向 NFC 令牌管理平台请求 NFC 令牌对应的用户的第三方支付平台账号信息；一个具体的例子为：请求处理模块 710 通过调用 NFC 令牌管理平台提供的接口将 NFC 令牌传输给 NFC 令牌管理平台，并从该接口的返回值中获得该用户的第三方支付平台账号信息。

作为示例，请求处理模块 710 可以先对其接收到的支付请求进行验证（如验证该支付请求是否为有效的支付请求等），并在验证通过的情况下，请求处理模块 710 向 NFC 令牌管理平台请求该 NFC 令牌对应的

用户的第三方支付平台账号信息。

支付处理模块 720 主要适于第三方支付平台根据请求而获得的用户的第三方支付平台账号信息进行支付处理，并通过银行平台向线下收费方发送支付信息。

5 具体的，在请求处理模块 710 基于请求而获得了用户的第三方支付平台账号信息之后，支付处理模块 720 可以向用户权益管理平台（如用户权益管理服务器）请求该用户的用户权益信息，如支付处理模块 720 通过调用用户权益管理平台提供的接口将该用户的第三方支付平台账号信息传输给用户权益管理平台，并接收用户权益管理平台返回的用户权益信息（如优惠券和/或积分等）。支付处理模块 720 可以在获得了用户权益管理平台返回的用户权益信息的基础上进行支付处理，如支付处理模块 720 根据用户权益信息计算用户针对本次订单而需要支付的金额（即当前支付金额）等。支付处理模块 720 通过在支付处理过程中引入用户权益信息，在很大程度上提高了线下支付结算的灵活性。

15 另外，支付处理模块 720 还可以将其接收到的订单信息提供给用户权益管理平台，如在支付处理之前或者在支付处理成功完成之后，支付处理模块 720 将订单信息提供给用户权益管理平台，以便于使用户权益管理平台可以针对用户的本次消费及时的更新用户当前的用户权益信息。支付处理模块 720 通过将订单信息提供给用户权益管理平台，使用户权益形成闭循环。

20 支付处理模块 720 可以根据用户预先为 NFC 支付设置的支付银行卡以及支付方式等信息按照现有的线上支付流程执行相应的操作，如支付处理模块 720 采用快捷支付方式进行支付扣款等。

25 支付处理模块 720 可以通过银行平台向线下收费方发送支付信息，以便于收费方完成本次费用收取。银行平台可以采用透传方式向线下收费方传输该支付信息。支付处理模块 720 所下发的支付信息除了包括当前支付金额之外，还可以包括订单号、本次使用的用户积分信息以及优惠信息等。本实施例不限制支付处理模块 720 向收费方下发的支付信息所包含的具体内容。

由上述描述可知，本实施例可以通过与用户移动设备进行一次信息交互（即传输 NFC 令牌的交互）即可完成费用支付以及用户权益核销等过程，使线下支付具有较好的便捷性。

实施例六、基于 NFC 的移动支付装置。

5 本实施例的装置可以设置于计算机设备中，且该装置可以设置于银行平台中，该装置的主要结构如图 8 所示。

图 8 中，基于 NFC 的移动支付装置主要包括：第二接收模块 800 以及控制模块 810。

10 第二接收模块 800 主要适于银行平台接收线下收费方发送来的包含 NFC 令牌和订单信息的支付请求。

具体的，第二接收模块 800 接收到的 NFC 令牌是由用户移动设备基于 NFC 传输至线下收费方，并由线下收费方将其产生的订单信息与该 NFC 令牌一起发送给银行平台的。另外，第二接收模块 800 接收到的 NFC 令牌可以是经过加密处理的 NFC 令牌，也可以为未经过加密处理的 NFC 令牌。

控制模块 810 主要适于在银行平台根据接收到的 NFC 令牌获取到相应的虚拟卡发卡行标识，根据该虚拟卡发卡行标识向第三方支付平台发送包含有 NFC 令牌和订单信息的支付请求。

20 具体的，控制模块 810 根据第二接收模块 800 接收到的 NFC 令牌获得相应的虚拟卡发卡行标识的过程可以为：控制模块 810 在第二接收模块 800 接收到收单服务器传输来的 NFC 令牌和订单信息后，通过调用 NFC 令牌管理平台提供的接口来获得 NFC 令牌对应的虚拟卡发卡行标识，即控制模块 810 通过调用 NFC 令牌管理平台提供的接口将上述 NFC 令牌传输给 NFC 令牌管理平台，以请求获得虚拟卡发卡行标识，
25 控制模块 810 从该接口返回的信息中获取虚拟卡发卡行标识。该接口返回的信息可以仅为虚拟卡发卡行标识，也可以为用户的第三支付平台账号以及虚拟卡发卡行标识，还可以为解密密钥以及预先设定的预定算法，还可以为解密处理后的 NFC 令牌等；控制模块 810 从接口返回的信息中获取虚拟卡发卡行标识的过程如上述实施例一中的描述，在此

不再详细说明。

控制模块 810 通常采用透传方式来向第三方支付平台发送包括 NFC 令牌和订单信息的支付请求。

实施例七、基于 NFC 的移动支付装置。

5 本实施例的装置可以设置于计算机设备中，且该装置可以设置于 NFC 令牌管理平台中，该装置的主要结构如图 9 所示。

图 9 中，基于 NFC 的移动支付装置主要包括：第三接收模块 900、虚拟卡管理模块 910 以及令牌管理模块 920。

10 第三接收模块 900 适于 NFC 令牌管理平台接收用户的虚拟卡开卡申请。

具体的，第三接收模块 900 接收到的虚拟卡开卡申请可以是用户移动设备直接传输来的，也可以是用户移动设备向第三方支付平台进行虚拟卡开卡申请，且第三方支付平台根据用户移动设备的申请而向 NFC 令牌管理平台传输的虚拟卡开卡申请。

15 虚拟卡管理模块 910 主要适于 NFC 令牌管理平台为第三接收模块 900 接收到的虚拟卡开卡申请设置虚拟卡发卡行标识。

具体的，虚拟卡管理模块 910 为虚拟卡开卡申请而设置的虚拟卡发卡行识别码用于表征第三方支付平台，即虚拟卡管理模块 910 为用户开设的虚拟卡是针对第三方支付平台，且具有发卡行标识 (bin) 的卡，如
20 虚拟卡的 bin 属于银联 bin 等，通过该虚拟卡的 bin 可以确定出该虚拟卡是针对第三方支付平台的。虚拟卡管理模块 910 为用户开设的该虚拟卡可以没有对应的真实存在的实物卡片，然而，虚拟卡管理模块 910 可以参考目前的银行卡（如银联卡）的相关环节对虚拟卡的申请以及管理等环节进行维护管理。当然，本实施例也不排除虚拟卡管理模块 910 为用
25 户开设的该虚拟卡存在与之对应的真实存在的实物卡片的可能性。虚拟卡管理模块 910 可以为一个用户开设一张或者多张虚拟卡。

令牌管理模块 920 主要适于 NFC 令牌管理平台根据用户的第三方支付平台账号信息和虚拟卡发卡行标识生成 NFC 令牌，并下发给用户移动设备。

具体的，令牌管理模块 920 可以利用预定算法对包括用户的第三方支付平台账号和虚拟卡发卡行识别码在内的信息进行计算，从而为该用户生成 NFC 令牌，令牌管理模块 920 可以对该 NFC 令牌进行加密处理，并将加密处理后的 NFC 令牌下发给用户移动设备；令牌管理模块 5 920 也可以不对 NFC 令牌进行加密处理，而是直接将其计算生成的 NFC 令牌下发给用户移动设备。令牌管理模块 920 可以直接将 NFC 令牌下发给用户移动设备，也可以将 NFC 令牌管理平台通过第三方支付平台下发给用户移动设备。

令牌管理模块 920 生成的 NFC 令牌可以存在使用限制，如 NFC 令牌 10 具有时效性和/或地域有效性和/或使用次数有效性等，具体请参见上述实施例一中的描述。

令牌管理模块 920 可以根据银行平台以及第三方支付平台的请求而向银行平台以及第三方支付平台返回与 NFC 令牌相关的信息，如令牌管理模块 920 根据来自银行平台的 NFC 令牌向银行平台返回虚拟卡发卡行标识；再如令牌管理模块 920 根据来自第三方支付平台的 NFC 令牌向 15 第三方支付平台返回用户的第三方支付账号信息等。另外，令牌管理模块 920 在根据银行平台以及第三方支付平台的请求而向银行平台以及第三方支付平台返回与 NFC 令牌相关的信息的过程中，可以根据 NFC 令牌的使用限制对接收到的 NFC 令牌进行有效性验证，在有效性验证 20 通过的情况下，令牌管理模块 920 向银行平台以及第三方支付平台返回与 NFC 令牌相关的信息，而在有效性验证失败的情况下，令牌管理模块 920 可以要求用户重新申请 NFC 令牌。

令牌管理模块 920 不仅可以在用户申请虚拟卡的过程中，为用户生成 NFC 令牌，还可以在用户具有虚拟卡之后，根据用户的申请而为用 25 户动态生成 NFC 令牌。具体请参见上述实施例一中的描述，在此不再详细说明。

需要注意的是，本发明可以在软件和/或者软件与硬件的组合物中被实施，例如，本发明的各个装置可采用专用集成电路 (ASIC) 或者任何其他类似硬件设备来实现。在一个实施例中，本发明的软件程序可

以通过处理器执行以实现上文所述步骤或功能。同样地，本发明的软件程序（包括相关的数据结构）可以被存储到计算机可读记录介质中，例如，RAM 存储器、磁或者光驱动器或软磁盘及类似设备。另外，本发明的一些步骤或功能可采用硬件来实现，例如，作为与处理器配合
5 从而执行各个步骤或功能的电路。

对于本领域技术人员而言，显然，本发明不限于上述示范性实施例的细节，而且在不背离本发明的精神或基本特征的情况下，能够以其他的具
10 体的形式实现本发明。因此，无论从哪一方面来看，均应该将实施例看作是示范性的，而且是非限制性的，本发明的范围由所附权利要求要求而不是上述说明来限定，因此，旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本发明内。不应该将权利要求中的任何附图标记视为限制所涉及的权利要求。此外，显然“包括”一词不排除其他单元或步骤，单数不排除复数。系统权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第一以
15 及第二等词语用来表示名称，而并不表示任何特定顺序。

虽然前面特别示出并且描述了示例性实施例，但是本领域技术人员将会理解的是，在不背离权利要求书的精神和范围的情况下，在其形式和细节方面可以有所变化。这里所寻求的保护在所附权利要求书中做了阐述。

权 利 要 求 书

1、一种基于 NFC 的移动支付方法，其中，该方法包括以下步骤：

5 第三方支付平台接收银行平台发送来的包含近场通讯 NFC 令牌和订单信息的支付请求，其中，所述 NFC 令牌由用户移动设备基于 NFC 传输至线下收费方，并经由线下收费方将 NFC 令牌和订单信息传输至银行平台；

第三方支付平台向 NFC 令牌管理平台请求所述 NFC 令牌对应的用户的第三方支付平台账号信息；

10 第三方支付平台根据所述请求而获得的用户的第三方支付平台账号信息进行支付处理，并通过银行平台向线下收费方发送支付信息。

2、根据权利要求 1 所述的方法，其中：

所述 NFC 令牌是 NFC 令牌管理平台根据用户的虚拟卡开卡申请而生成并下发给用户移动设备的 NFC 令牌；或者

15 所述 NFC 令牌是 NFC 令牌管理平台根据已具有虚拟卡的用户的 NFC 令牌动态申请而生成并下发给用户移动设备的 NFC 令牌。

3、根据权利要求 1 所述的方法，其中：

20 所述 NFC 令牌是 NFC 令牌管理平台利用预定算法对包含有用户的第三方支付平台账号和虚拟卡发卡行识别码在内的信息进行计算获得的；或者

所述 NFC 令牌是 NFC 令牌管理平台利用预定算法对包含有用户的第三方支付平台账号以及虚拟卡发卡行识别码在内的信息进行计算并加密获得的；

其中，所述虚拟卡发卡行识别码用于表征第三方支付平台。

25 4、根据权利要求 3 所述的方法，其中，所述第三方支付平台接收银行平台发送来的包含近场通讯 NFC 令牌和订单信息的支付请求包括：

在银行平台根据接收到的 NFC 令牌获取到相应的虚拟卡发卡行标识的情况下，银行平台根据该虚拟卡发卡行标识向第三方支付平台发

送支付请求。

5、根据权利要求 4 所述的方法，其中，所述银行平台根据接收到的 NFC 令牌获取到相应的虚拟卡发卡行标识包括：

5 银行平台向 NFC 令牌管理平台发送所述 NFC 令牌，并接收 NFC 令牌管理平台返回的所述 NFC 令牌对应的虚拟卡发卡行标识；或者

银行平台向 NFC 令牌管理平台发送所述 NFC 令牌，并接收 NFC 令牌管理平台返回的所述 NFC 令牌的密钥以及预定算法，银行平台根据所述密钥和预定算法对 NFC 令牌进行解密以及计算处理，并从处理结果中获得虚拟卡发卡行标识；或者

10 银行平台向 NFC 令牌管理平台发送所述 NFC 令牌，NFC 令牌管理平台对所述 NFC 令牌进行解密和计算处理，并向银行平台返回解密和计算处理结果信息，银行平台从所述处理结果信息中获取虚拟卡发卡行标识。

15 6、根据权利要求 1 所述的方法，其中，所述第三方支付平台向 NFC 令牌管理平台请求所述 NFC 令牌对应的用户的第三方支付平台账号信息包括：

NFC 令牌管理平台对来自所述第三方支付平台的 NFC 令牌进行有效性验证，并在有效性验证通过的情况下，向第三方支付平台返回所述 NFC 令牌对应的用户的第三方支付平台账号信息；

20 其中，所述有效性验证包括：时效性验证、地域有效性以及使用次数有效性验证中的至少一个。

7、根据权利要求 1 至 6 中任一权利要求所述的方法，其中，所述第三方支付平台根据所述请求而获得的用户的第三方支付平台账号信息进行支付处理包括：

25 第三方支付平台根据所述用户的第三方支付平台账号信息向用户权益管理平台请求用户权益信息，并根据用户权益管理平台返回的用户权益信息计算当前支付金额。

8、一种基于 NFC 的移动支付方法，其中，该方法包括以下步骤：

银行平台接收线下收费方发送来的包含 NFC 令牌和订单信息的支

付请求，其中，所述 NFC 令牌由用户移动设备基于 NFC 传输至线下收费方，所述订单信息由线下收费方产生；

在银行平台根据接收到的 NFC 令牌获取到相应的虚拟卡发卡行标识的情况下，银行平台根据该虚拟卡发卡行标识向第三方支付平台发送支付请求。

9、根据权利要求 8 所述的方法，其中，所述银行平台根据接收到的 NFC 令牌获取到相应的虚拟卡发卡行标识包括：

银行平台向 NFC 令牌管理平台发送所述 NFC 令牌，并接收 NFC 令牌管理平台返回的所述 NFC 令牌对应的虚拟卡发卡行标识；或者

银行平台向 NFC 令牌管理平台发送所述 NFC 令牌，并接收 NFC 令牌管理平台返回的所述 NFC 令牌的密钥以及预定算法，银行平台根据所述密钥和预定算法对 NFC 令牌进行解密以及计算处理，并从处理结果中获得虚拟卡发卡行标识；或者

银行平台向 NFC 令牌管理平台发送所述 NFC 令牌，NFC 令牌管理平台对所述 NFC 令牌进行解密和计算处理，并向银行平台返回解密和计算处理结果信息，银行平台从所述处理结果信息中获取虚拟卡发卡行标识。

10、一种基于 NFC 的移动支付方法，其中，该方法包括以下步骤：

NFC 令牌管理平台接收用户的虚拟卡开卡申请；

NFC 令牌管理平台为所述虚拟卡开卡申请设置虚拟卡发卡行标识；

NFC 令牌管理平台根据用户的第三方支付平台账号信息和虚拟卡发卡行标识生成 NFC 令牌，并下发给用户移动设备；

其中，所述虚拟卡发卡行识别码用于表征第三方支付平台。

11、根据权利要求 10 所述的方法，其中，所述 NFC 令牌管理平台根据用户的第三方支付平台账号信息和虚拟卡发卡行标识生成 NFC 令牌包括：

NFC 令牌管理平台利用预定算法对包含有用户的第三方支付平台账号和虚拟卡发卡行识别码在内的信息进行计算生成 NFC 令牌；或者

NFC 令牌管理平台利用预定算法对包含有用户的第三方支付平台账号和虚拟卡发卡行识别码在内的信息进行计算并加密生成 NFC 令牌。

12、根据权利要求 10 所述的方法，其中，所述方法还包括：

NFC 令牌管理平台对来自所述第三方支付平台的 NFC 令牌进行有效性验证，并在有效性验证通过的情况下，向第三方支付平台返回所述 NFC 令牌对应的用户的第三方支付平台账号信息；

其中，所述有效性验证包括：时效性验证、地域有效性以及使用次数有效性验证中的至少一个。

13、一种基于 NFC 的移动支付装置，其中，该装置包括：

10 第一接收模块，适于第三方支付平台接收银行平台发送来的包含近场通讯 NFC 令牌和订单信息的支付请求，其中，所述 NFC 令牌由用户移动设备基于 NFC 传输至线下收费方，并经由线下收费方将 NFC 令牌和订单信息传输至银行平台；

请求处理模块，适于第三方支付平台向 NFC 令牌管理平台请求所述 NFC 令牌对应的用户的第三方支付平台账号信息；

支付处理模块，适于第三方支付平台根据所述请求而获得的用户的第三方支付平台账号信息进行支付处理，并通过银行平台向线下收费方发送支付信息。

14、根据权利要求 13 所述的装置，其中：

20 所述 NFC 令牌是 NFC 令牌管理平台根据用户的虚拟卡开卡申请而生成并下发给用户移动设备的 NFC 令牌；或者

所述 NFC 令牌是 NFC 令牌管理平台根据已具有虚拟卡的用户的 NFC 令牌动态申请而生成并下发给用户移动设备的 NFC 令牌。

25 15、根据权利要求 13 或 14 所述的装置，其中，所述支付处理模块具体适于：

第三方支付平台根据所述用户的第三方支付平台账号信息向用户权益管理平台请求用户权益信息，并根据用户权益管理平台返回的用户权益信息计算当前支付金额。

16、一种基于 NFC 的移动支付装置，其中，该装置包括：

第二接收模块，适于银行平台接收线下收费方发送来的包含 NFC 令牌和订单信息的支付请求，其中，所述 NFC 令牌由用户移动设备基于 NFC 传输至线下收费方，所述订单信息由线下收费方产生；

5 控制模块，适于在银行平台根据接收到的 NFC 令牌获取到相应的虚拟卡发卡行标识，根据该虚拟卡发卡行标识向第三方支付平台发送支付请求，其中，所述虚拟卡发卡行识别码用于表征第三方支付平台。

17、根据权利要求 16 所述的装置，其中，所述第二接收模块具体适于：

10 银行平台向 NFC 令牌管理平台发送所述 NFC 令牌，并接收 NFC 令牌管理平台返回的所述 NFC 令牌对应的虚拟卡发卡行标识；或者

15 银行平台向 NFC 令牌管理平台发送所述 NFC 令牌，并接收 NFC 令牌管理平台返回的所述 NFC 令牌的密钥以及预定算法，银行平台根据所述密钥和预定算法对 NFC 令牌进行解密以及计算处理，并从处理结果中获得虚拟卡发卡行标识；或者

银行平台向 NFC 令牌管理平台发送所述 NFC 令牌，NFC 令牌管理平台对所述 NFC 令牌进行解密和计算处理，并向银行平台返回解密和计算处理结果信息，银行平台从所述处理结果信息中获取虚拟卡发卡行标识。

20 18、一种基于 NFC 的移动支付装置，其中，所述装置包括：

第三接收模块，适于 NFC 令牌管理平台接收用户的虚拟卡开卡申请；

虚拟卡管理模块，适于 NFC 令牌管理平台为所述虚拟卡开卡申请设置虚拟卡发卡行标识；

25 令牌管理模块，适于 NFC 令牌管理平台根据用户的第三方支付平台账号信息和虚拟卡发卡行标识生成 NFC 令牌，并下发给用户移动设备；

其中，所述虚拟卡发卡行识别码用于表征第三方支付平台。

19、根据权利要求 18 所述的装置，其中，所述令牌管理模块具体

适于：

NFC 令牌管理平台利用预定算法对包含有用户的第三方支付平台账号和虚拟卡发卡行识别码在内的信息进行计算生成 NFC 令牌；或者

5 NFC 令牌管理平台利用预定算法对包含有用户的第三方支付平台账号和虚拟卡发卡行识别码在内的信息进行计算并加密生成 NFC 令牌。

20、根据权利要求 18 或 19 所述的装置，其中，所述令牌管理模块还适于：

10 NFC 令牌管理平台对来自所述第三方支付平台的 NFC 令牌进行有效性验证，并在有效性验证通过的情况下，向第三方支付平台返回所述 NFC 令牌对应的用户的第三方支付平台账号信息；

其中，所述有效性验证包括：时效性验证、地域有效性以及使用次数有效性验证中的至少一个。

15 21. 一种计算机可读存储介质，所述计算机可读存储介质包括计算机指令，当所述计算机指令被执行时，如权利要求 1 至 12 中任一项所述的方法被执行。

22. 一种计算机程序产品，当所述计算机程序产品被执行时，如权利要求 1 至 12 中任一项所述的方法被执行。

20 23. 一种计算机设备，所述计算机设备包括存储器和处理器，所述存储器中存储有计算机指令，所述处理器被配置来通过执行所述计算机指令以执行如权利要求 1 至 12 中任一项所述的方法。

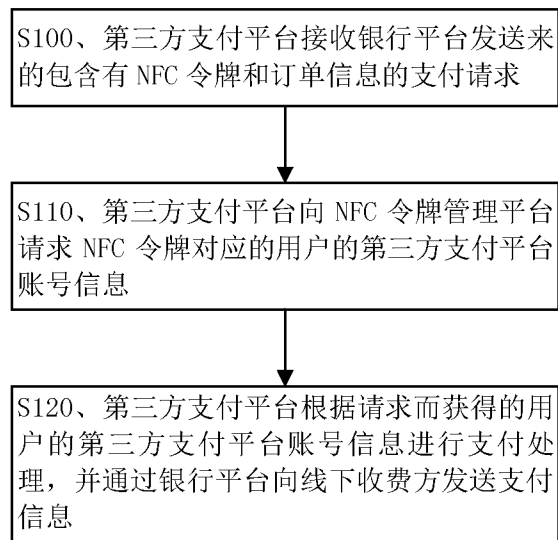


图 1

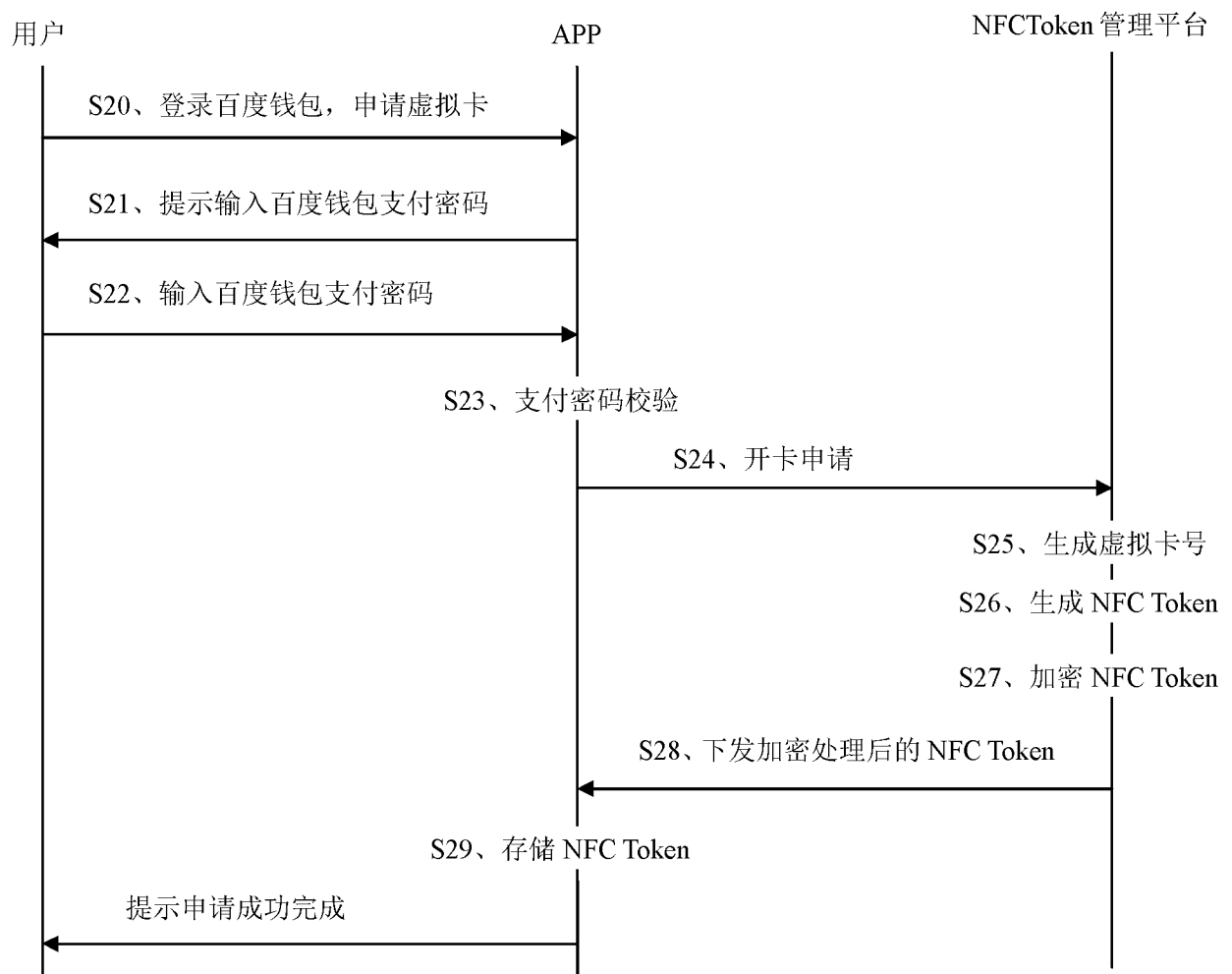


图 2

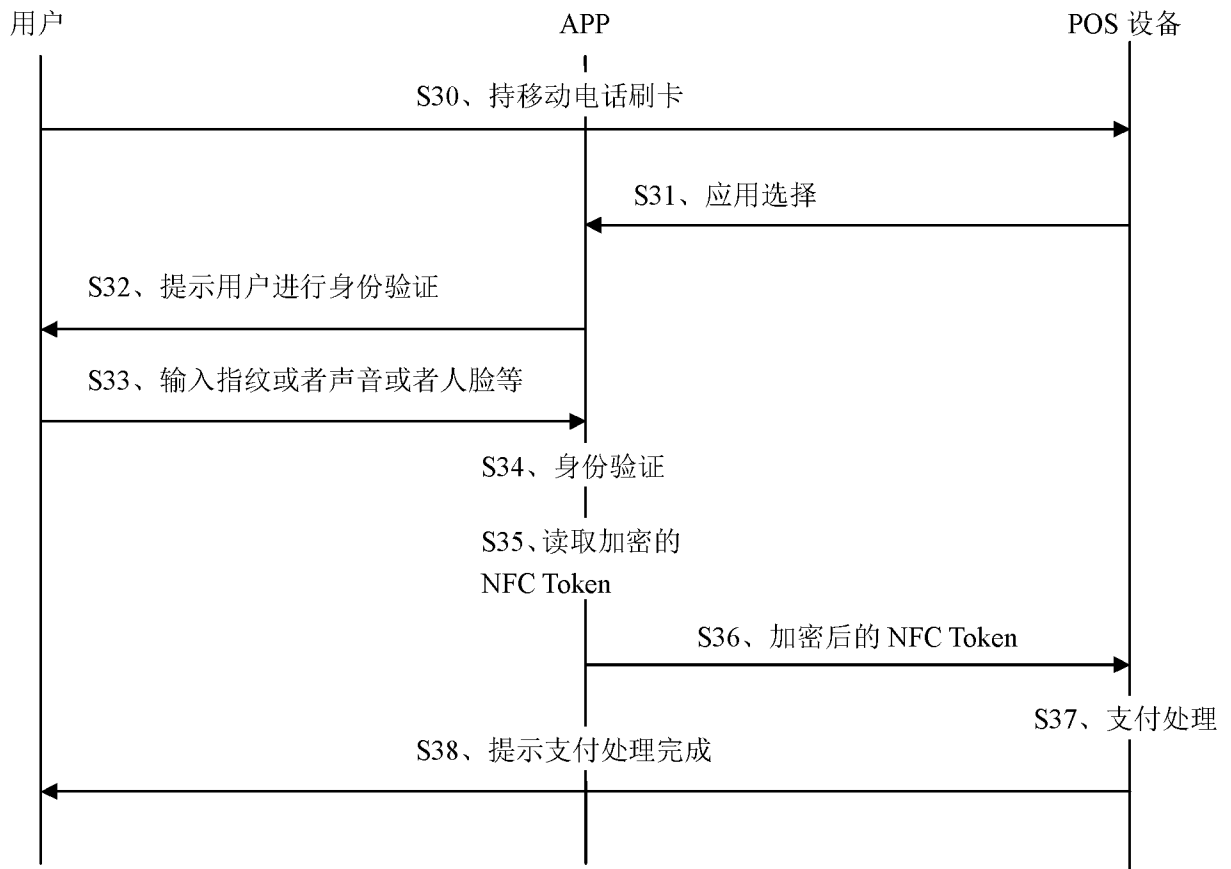


图 3

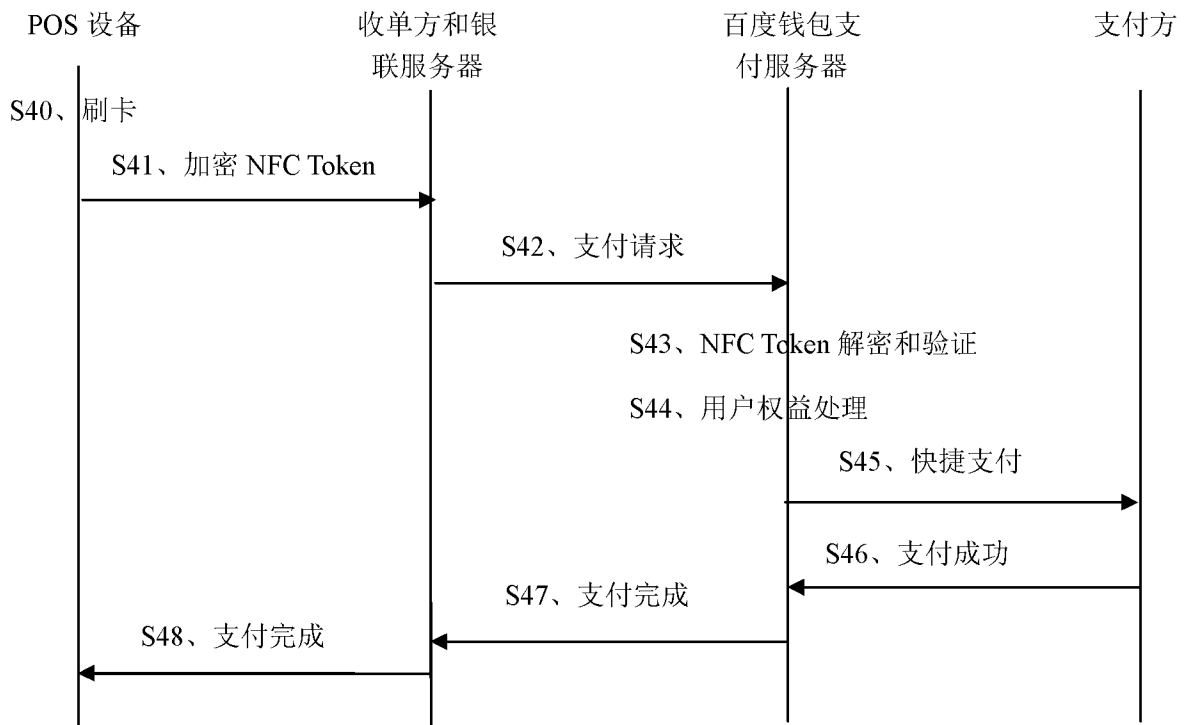


图 4

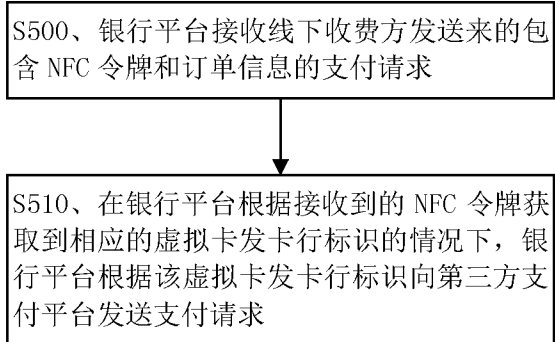


图 5

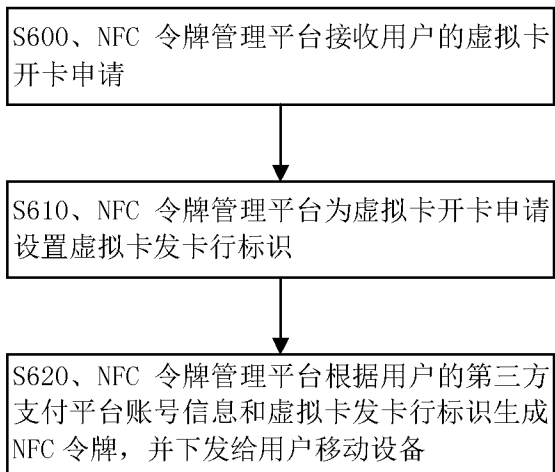


图 6

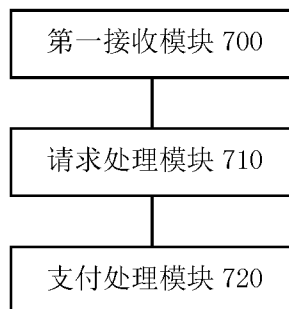


图 7



图 8



图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/094730

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/32 (2012.01) i; G06Q 20/40 (2012.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Databases: CNABS, DWPI, SIPOABS, CNKI

Search Terms: near field communication, NFC, token, payment, third party, account number

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015127547 A1 (POWELL, G.L. et al.), 07 May 2015 (07.05.2015), see description, paragraphs 0033-0037 and 0103-0128, and figures 2-3	1-23
X	US 2015199689 A1 (KUMNICK, P. et al.), 16 July 2015 (16.07.2015), see description, paragraphs 0027-0033 and 0054-0102, and figures 1-2	1-23
PX	CN 105046486 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.), 11 November 2015 (11.11.2015), see claims 1-20	1-23

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 23 February 2016 (23.02.2016)	Date of mailing of the international search report 01 March 2016 (01.03.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer ZOU, Bin Telephone No.: (86-10) 62412066

International application No.
PCT/CN2015/094730

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2015/094730

A. 主题的分类

G06Q 20/32(2012.01)i; G06Q 20/40(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

数据库: CNABS, DWPI, SIPOABS, CNKI 检索词: 近场通信, 令牌, 支付, 第三方, 账号, NFC, token, payment, third party, account number

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	US 2015127547 A1 (POWELL, GLENN LEON等) 2015年 5月 7日 (2015 - 05 - 07) 参见说明书第0033-0037, 0103-0128段, 图2-3	1-23
X	US 2015199689 A1 (KUMNICK, PHILLIP等) 2015年 7月 16日 (2015 - 07 - 16) 参见说明书第0027-0033, 0054-0102段, 图1-2	1-23
PX	CN 105046486 A (百度在线网络技术北京有限公司) 2015年 11月 11日 (2015 - 11 - 11) 参见权利要求1-20	1-23

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 2月 23日

国际检索报告邮寄日期

2016年 3月 1日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

授权官员

邹斌

电话号码 (86-10)62412066

国际申请号
PCT/CN2015/094730

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
US	2015127547	A1	2015年 5月 7日	WO	2015054697	A1	2015年 4月 16日
US	2015199689	A1	2015年 7月 16日	无			
CN	105046486	A	2015年 11月 11日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)