(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108009820 B
(45)授权公告日 2020.08.25

(21)申请号 201711349196.5
(22)申请日 2017.12.15
(65)同一申请的已公布的文献号
申请公布号 CN 108009820 A
(43)申请公布日 2018.05.08
(73)专利权人 恒宝股份有限公司
地址 212355 江苏省镇江市丹阳市横塘工业区
(72)发明人 肖永兴 孔索红
(74)专利代理机构 北京卓特专利代理事务所（普通合伙）11572
代理人 陈变花
(51)Int.Cl.
G06F 21/30(2013.01)

审查员 刘晶

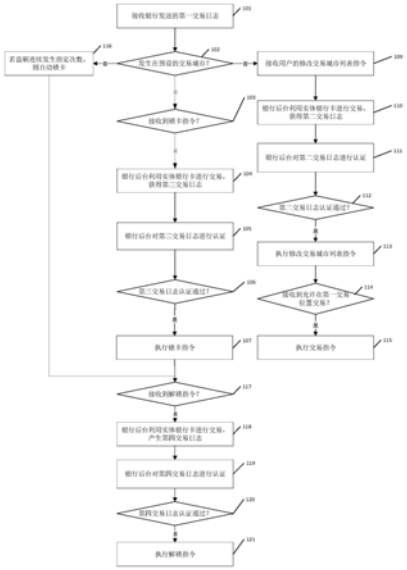
权利要求书3页 说明书6页 附图3页

(54)发明名称

移动终端及基于移动终端的银行卡的防盗刷方法

(57)摘要

本申请提供一种移动终端及基于移动终端的银行卡的防盗刷方法，方法包括：接收银行发送的银行卡的第一交易日志；若第一交易位置不属于银行卡预设的交易城市列表，则接收用户输入的指令；若接收到修改交易城市列表的指令，则利用实体银行卡通过移动终端的无线通信模块进行交易，形成第二交易日志；对第二交易日志进行认证；若第二交易日志的认证通过，则执行修改交易城市列表的指令。本申请利用移动终端的近场无线通信对实体银行卡进行操作获取凭证，快速而方便的证明真卡与伪卡的非同一性，并通过移动终端上的微信公众号或银行客户端对银行卡进行锁卡操作，避免用户通过电话或柜台证明银行卡和用户不在交易所在地导致的延迟和损失。



CN 108009820 B

1.一种基于移动终端的银行卡的防盗刷方法,其特征在于,所述移动终端包括所述银行卡所属的银行的银行后台,包括如下步骤:

接收银行发送的银行卡的第一交易日志,所述第一交易日志包括第一交易位置和第一交易时间;

若所述第一交易位置不属于银行卡预设的交易城市列表,则接收用户输入的指令;

若接收到修改交易城市列表的指令,则利用实体银行卡通过所述移动终端的无线通信模块进行交易,记录实体银行卡的交易位置和交易时间,分别作为第二交易位置和第二交易时间,所述第二交易位置和所述第二交易时间形成第二交易日志;

对所述第二交易日志进行认证;

若所述第二交易日志的认证通过,则执行所述修改交易城市列表的指令,将第一交易位置所属的城市列表加入交易城市列表中进行交易;

其中若银行卡发生盗刷,则通过银行卡位置的取证以及上传从而进行证据的采集,其中在修改交易城市列表的过程中,同样进行银行卡位置的取证,银行卡位置的取证具体包括以下步骤:银行后台通过所述无线通信模块向实体银行卡发送APDU指令,其中所述APDU指令为交易金额为0的认证,银行后台通过无线通信模块接收实体银行卡返回的对APDU指令的交易数据;银行后台使用公钥和指数对脱机交易产生的交易数据进行加密,获得加密数据;银行后台验证加密数据是否符合正确的数据格式;若格式验证通过,则银行后台获取加密数据中的部分数据,并利用部分数据和产生的随机数计算哈希值,判断哈希值与加密数据是否相同;若哈希值与加密数据相同,则所属第二交易日志的认证通过。

2.根据权利要求1所述的基于移动终端的银行卡的防盗刷方法,其特征在于,还包括:接收并执行用户输入的锁卡或继续交易指令。

3.根据权利要求1所述的基于移动终端的银行卡的防盗刷方法,其特征在于,所述银行后台是银行卡所属银行的微信公众号或安装在所述移动终端上的银行客户端。

4.根据权利要求1所述的基于移动终端的银行卡的防盗刷方法,其特征在于,利用实体银行卡进行交易包括如下步骤:

通过所述无线通信模块向实体银行卡发送APDU指令,所述APDU指令为交易金额为0的GPO认证;

通过所述无线通信模块接收实体银行卡返回的对所述APDU指令的交易返回数据。

5.根据权利要求4所述的基于移动终端的银行卡的防盗刷方法,其特征在于,对所述第二交易日志进行认证包括如下步骤:

使用公钥和指数对脱机交易产生的交易数据进行加密,获得加密数据;

验证所述加密数据是否符合正确的数据格式;

若格式验证通过,则获取所述加密数据中的部分数据,并利用所述部分数据和产生的随机数计算哈希值;

判断所述哈希值与所述加密数据是否相同;

若所述哈希值与所述加密数据相同,则所述第二交易日志的认证通过。

6.根据权利要求1所述的基于移动终端的银行卡的防盗刷方法,其特征在于,还包括:

若所述第一交易位置属于银行卡预设的交易城市列表,则接收用户输入的指令;

若接收到锁卡指令,则利用实体银行卡通过所述移动终端的无线通信模块进行交易,

记录实体银行卡的交易位置和交易时间,分别作为第三交易位置和第三交易时间,所述第三交易位置和所述第三交易时间形成第三交易日志;所述无线通信模块为NFC模块、蓝牙模块或WIFI;

对所述第三交易日志进行认证;

若所述第三交易日志的认证通过,则

执行所述锁卡指令。

7.根据权利要求2或6所述的基于移动终端的银行卡的防盗刷方法,其特征在于,还包括:

接收用户输入的指令;

若接收到对所述银行卡的解锁指令,则利用实体银行卡通过所述移动终端的无线通信模块进行交易,记录实体银行卡的交易位置和交易时间,分别作为第四交易位置和第四交易时间,所述第四交易位置和所述第四交易时间形成第四交易日志;

对所述第四交易日志进行认证;

若所述第四交易日志的认证通过,则执行所述解锁指令。

8.一种移动终端,其特征在于,所述移动终端包括第一交易日志接收模块;

所述移动终端包括银行卡所属的银行的银行后台,所述银行后台包括用户指令接收模块、实体卡交易模块、第二交易日志认证模块、指令执行模块;

所述第一交易日志接收模块,用于接收银行发送的银行卡的第一交易日志,所述第一交易日志包括第一交易位置和第一交易时间;

所述用户指令接收模块用于接收用户输入的指令;

所述实体卡交易模块与所述用户指令接收模块连接,用于利用实体银行卡通过所述移动终端的无线通信模块进行交易,记录实体银行卡的交易位置和交易时间,分别作为第二交易位置和第二交易时间,所述第二交易位置和所述第二交易时间形成第二交易日志;所述无线通信模块为NFC模块、蓝牙模块或WIFI;

所述第二交易日志认证模块与所述实体卡交易模块连接,用于对所述第二交易日志进行认证;

指令执行模块与所述第二交易日志认证模块连接,用于响应于所述第二交易日志的认证通过而执行用户输入的指令,具体为执行修改交易城市列表从而完成交易;

其中所述实体卡交易模块包括APDU指令发送模块和交易数据接收模块,用于若发生银行卡的盗刷则进行银行卡位置的取证;其中银行卡位置的取证具体包括以下步骤:银行后台通过所述无线通信模块向实体银行卡发送APDU指令,其中所述APDU指令为交易金额为0的认证,银行后台通过无线通信模块接收实体银行卡返回的对APDU指令的交易数据;银行后台使用公钥和指数对脱机交易产生的交易数据进行加密,获得加密数据;银行后台验证加密数据是否符合正确的数据格式;若格式验证通过,则银行后台获取加密数据中的部分数据,并利用部分数据和产生的随机数计算哈希值,判断哈希值与加密数据是否相同;若哈希值与加密数据相同,则所属第二交易日志的认证通过;

所述APDU指令发送模块用于通过无线通信模块向实体银行卡发送APDU指令,所述APDU指令为交易金额为0的GPO认证;

所述交易数据接收模块用于通过所述无线通信模块接收实体银行卡返回的对所述

APDU指令的交易数据。

9.根据权利要求8所述的移动终端，其特征在于，所述第二交易日志认证模块包括交易数据接收模块、加密数据获取模块、格式验证模块、哈希值计算模块以及数据判断模块；

所述交易数据接收模块，用于通过所述无线通信模块接收所述交易数据；

所述加密数据获取模块与所述交易数据接收模块连接，用于使用公钥和指数对脱机交易产生的交易数据进行加密，获得加密数据；

所述格式验证模块与所述加密数据获取模块连接，用于验证所述加密数据是否符合正确的数据格式；

所述哈希值计算模块与所述格式验证模块和所述加密数据获取模块连接，用于响应于格式验证通过而获取所述加密数据中的部分数据，并利用所述部分数据和银行客户端产生的随机数计算哈希值；

所述数据判断模块与所述哈希值计算模块连接，用于判断所述哈希值与所述加密数据是否相同。

移动终端及基于移动终端的银行卡的防盗刷方法

技术领域

[0001] 本申请涉及通信技术领域，尤其涉及一种移动终端及基于移动终端的银行卡的防盗刷方法。

背景技术

[0002] 网上购物或刷卡消费等消费方式给生活带来了不少便利，但它同时也成为了不法分子的“猎物”，银行卡统一被盗刷。如果银行卡被盗刷，采用如下方法才能获得全额赔付：

[0003] 1、第一时间向发卡行电话挂失，避免盗刷损失进一步扩大。

[0004] 2、在异地盗刷情况下，持银行卡到本地的柜员机操作(查询、存取等)，用于固定电子证据，证明盗刷时银行卡和本人均在本地，不可能同一时间在异地刷卡消费。

[0005] 3、及时向公安机关报案，详述被盗刷情况，留好报警回执，用于证明银行卡仍由自己妥善保管，盗刷消费非本人所为。

[0006] 4、迅速与涉事银行联系，主动沟通后续赔偿事宜。

[0007] 但是，现有的盗刷处理方法具有一定的局限性。持卡人需要去柜员机进行操作方可得到凭条，在时间和空间上受到限制，无法及时获得证据，并且如果持卡人延误了对卡片盗刷时间的上报，可能出现银行不全额赔付盗刷金额的情况。

发明内容

[0008] 本申请的目的在于提供一种移动终端及基于移动终端的银行卡的防盗刷方法，方便持卡人及时认定盗刷现象，避免更大损失。

[0009] 为达到上述目的，本申请提供一种基于移动终端的银行卡的防盗刷方法，移动终端包括银行卡所属的银行的银行后台，包括如下步骤：接收银行发送的银行卡的第一交易日志，第一交易日志包括第一交易位置和第一交易时间；若第一交易位置不属于银行卡预设的交易城市列表，则接收用户输入的指令；若接收到修改交易城市列表的指令，则利用实体银行卡通过移动终端的无线通信模块进行交易，记录实体银行卡的交易位置和交易时间，分别作为第二交易位置和第二交易时间，第二交易位置和第二交易时间形成第二交易日志；对第二交易日志进行认证；若第二交易日志的认证通过，则执行修改交易城市列表的指令。

[0010] 如上的，其中，还包括：接收并执行用户输入的锁卡或继续交易指令。

[0011] 如上的，其中，银行后台是银行卡所属银行的微信公众号或安装在移动终端上的银行客户端。

[0012] 如上的，其中，利用实体银行卡进行交易包括如下步骤：通过无线通信模块向实体银行卡发送APDU指令，APDU指令为交易金额为0的GPO认证；通过无线通信模块接收实体银行卡返回的对APDU指令的交易返回数据。

[0013] 如上的，其中，对第二交易日志进行认证包括如下步骤：使用公钥和指数对脱机交易产生的交易数据进行加密，获得加密数据；验证加密数据是否符合正确的数据格式；若格

式验证通过，则获取加密数据中的部分数据，并利用部分数据和产生的随机数计算哈希值；判断哈希值与加密数据是否相同；若哈希值与加密数据相同，则第二交易日志的认证通过。

[0014] 如上的，其中，还包括：若第一交易位置属于银行卡预设的交易城市列表，则接收用户输入的指令；若接收到锁卡指令，则利用实体银行卡通过移动终端的无线通信模块进行交易，记录实体银行卡的交易位置和交易时间，分别作为第三交易位置和第三交易时间，第三交易位置和第三交易时间形成第三交易日志；无线通信模块为NFC模块、蓝牙模块或WIFI；对第三交易日志进行认证；若第三交易日志的认证通过，则执行锁卡指令。

[0015] 如上的，其中，若第一交易位置不属于银行卡预设的交易城市列表，并且银行卡连续被使用指定次数并且连续指定次数未接收到用户的锁卡指令，则自动锁卡。

[0016] 如上的，其中，还包括：自自动锁卡起指定时间后自动对银行卡进行解锁。

[0017] 如上的，其中，还包括：接收用户输入的指令；若接收到对银行卡的解锁指令，则利用实体银行卡通过移动终端的无线通信模块进行交易，记录实体银行卡的交易位置和交易时间，分别作为第四交易位置和第四交易时间，第四交易位置和第四交易时间形成第四交易日志；对第四交易日志进行认证；若第四交易日志的认证通过，则执行解锁指令。

[0018] 本申请还提供了一种移动终端，移动终端包括第一交易日志接收模块；移动终端包括银行卡所属的银行的银行后台，银行后台包括用户指令接收模块、实体卡交易模块、第二交易日志认证模块、指令执行模块；第一交易日志接收模块，用于接收银行发送的银行卡的第一交易日志，第一交易日志包括第一交易位置和第一交易时间；用户指令接收模块用于接收用户输入的指令；实体卡交易模块与用户指令接收模块连接，用于利用实体银行卡通过移动终端的无线通信模块进行交易，记录实体银行卡的交易位置和交易时间，分别作为第二交易位置和第二交易时间，第二交易位置和第二交易时间形成第二交易日志；无线通信模块为NFC模块、蓝牙模块或WIFI；第二交易日志认证模块与实体卡交易模块连接，用于对第二交易日志进行认证；指令执行模块，用于响应于第二交易日志的认证通过而执行用户输入的指令。

[0019] 如上的，其中，实体卡交易模块包括APDU指令发送模块和交易数据接收模块；APDU指令发送模块用于通过无线通信模块向实体银行卡发送APDU指令，APDU指令为交易金额为0的GPO认证；交易数据接收模块用于通过无线通信模块接收实体银行卡返回的对APDU指令的交易数据。

[0020] 如上的，其中，第二交易日志认证模块包括交易数据接收模块、加密数据获取模块、格式验证模块、哈希值计算模块以及数据判断模块；交易数据接收模块，用于通过无线通信模块接收交易数据；加密数据获取模块与交易数据接收模块连接，用于使用公钥和指数对脱机交易产生的交易数据进行加密，获得加密数据；格式验证模块与加密数据获取模块连接，用于验证加密数据是否符合正确的数据格式；哈希值计算模块与格式验证模块和加密数据获取模块连接，用于响应于格式验证通过而获取加密数据中的部分数据，并利用部分数据和银行客户端产生的随机数计算哈希值；数据判断模块与哈希值计算模块连接，用于判断哈希值与加密数据是否相同。

[0021] 如上的，其中，银行后台还包括自动锁卡模块，用于响应于第一交易位置不属于银行卡预设的交易城市列表，并且银行卡连续被使用指定次数并且连续指定次数未接收到用户的锁卡指令而执行自动锁卡。

[0022] 如上的，其中，银行后台还包括自动解锁模块与自动锁卡模块连接，用于自自动锁卡起指定时间后自动对银行卡进行解锁。

[0023] 本申请利用移动终端的NFC、蓝牙或wifi等近场无线通信对实体银行卡进行操作获取凭证，快速而方便的证明真卡与伪卡的非同一性，并通过移动终端上的微信公众号或银行客户端对银行卡进行锁卡操作，避免用户通过电话或柜台证明银行卡和用户不在交易所在地导致的延迟和损失。

附图说明

[0024] 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，对于本领域技术人员来讲，还可以根据这些附图获得其他的附图。

[0025] 图1为本申请实施例提供的基于移动终端的银行卡的防盗刷方法的流程图；

[0026] 图2为本申请实施例提供的移动终端的结构图；

[0027] 图3为本申请实施例提供的银行后台的结构图；

[0028] 图4为本申请实施例提供的实体卡交易模块的结构图；

[0029] 图5是本申请实施例提供的第二交易日志认证模块的结构图。

具体实施方式

[0030] 下面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，本领域技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0031] 本申请中，移动终端包括银行卡所属的银行的银行后台。具体地，银行后台可以是微信公众号或安装移动终端上的银行客户端，银行后台中预设了银行卡的交易城市列表。

[0032] 如果刷卡消费发生在交易城市列表内的城市的刷卡可完成交易。如果消费发生于银行后台设置的交易城市列表外的城市，银行可以直接制止消费行为，银行卡持有人不会有任何经济损失，银行也不用处理这种事件。此方案对于较难解决的网上盗刷有很重要的作用。

[0033] 移动终端具有近场无线通信模块，移动终端只能在短距离内进行无线通信。无线通信模块可以为NFC模块、蓝牙模块或WIFI中的一种或多种。

[0034] 实施例一

[0035] 图1为本申请实施例提供的基于移动终端的银行卡的防盗刷方法的流程图。如图1所示，防盗刷方法包括：

[0036] 步骤101：当银行卡被操作(如通过POS机消费或手机APP消费等)时，移动终端接收银行发送的第一交易日志，第一交易日志包括第一交易位置和第一交易时间。

[0037] 步骤102：银行后台可根据第一交易位置判断本次交易所属的城市是否属于预设的交易城市，并告知用户(银行卡持卡人)。

[0038] 若本次交易是银行后台预设的交易城市列表外的城市的刷卡，即异地消费。如果

是用户认可的消费，则用户可通过银行后台修改交易城市列表，将第一位置所属的城市列入交易城市列表再进行交易。在此情况下，移动终端执行如下步骤：

[0039] 步骤109：银行后台接收用户输入的修改交易城市列表的指令。

[0040] 步骤110：银行后台利用实体银行卡通过移动终端的无线通信模块进行交易，记录实体银行卡的交易位置和交易时间，分别作为第二交易位置和第二交易时间，第二交易位置和第二交易时间形成第二交易日志。

[0041] 具体地，利用实体银行卡进行交易包括如下步骤：

[0042] 银行后台通过无线通信模块向实体银行卡发送APDU指令，APDU指令为交易金额为0的GPO认证。

[0043] 银行后台通过无线通信模块接收实体银行卡返回的对APDU指令的交易数据。

[0044] 该步骤中，银行卡持有人通过移动终端的近场通信功能证明实体卡和移动终端在一起，并且记录了实体卡所在的位置，银行卡持有人无需去银行柜台或ATM机即可完成实体卡所在位置的取证，方便快捷。

[0045] 步骤111：银行后台对第二交易日志进行认证，具体包括如下步骤：

[0046] 银行后台使用公钥和指数对脱机交易产生的交易数据进行加密，获得加密数据。

[0047] 银行后台验证加密数据是否符合正确的数据格式。

[0048] 若格式验证通过，则银行后台获取加密数据中的部分数据，并利用部分数据和产生的随机数计算哈希值。

[0049] 判断哈希值与加密数据是否相同。

[0050] 若哈希值与加密数据相同，则第二交易日志的认证通过。

[0051] 步骤112：判断第二交易日志的认证是否通过。

[0052] 若认证通过，则执行步骤113：执行修改交易城市列表的指令。

[0053] 修改完交易城市列表后，用户可根据实际情况指示允许在第一交易位置进行交易。包括如下步骤：

[0054] 步骤114：判断是否接收到允许在第一交易位置进行交易的指令。

[0055] 若接收到允许在第一交易位置进行交易的指令，则执行步骤115：银行后台向银行发送允许在第一交易位置进行交易的指令，第一交易位置的操作人即可进行交易。

[0056] 若第一交易位置不属于银行卡预设的交易城市列表，并且银行卡连续被使用指定次数并且连续该指定次数用户都没有指示锁卡，则银行后台可以进行自动锁卡(步骤116)，以防银行卡被再次盗刷。在异地盗刷导致自动锁卡的情况下，用户可以在银行后台上预设自动解锁，即自自动锁卡起指定时间后银行后台自动对银行卡进行解锁，避免用户通过银行柜台或电话进行解锁带来的麻烦，并可以避免影响用户的正常使用。

[0057] 无论是通过手动锁卡或是自动锁卡，用户均可通过银行后台进行手动解锁。具体包括如下步骤：

[0058] 步骤117：银行后台判断是否接收到解锁指令。

[0059] 若接收到用户的解锁指令，则执行步骤118：银行后台利用实体银行卡通过移动终端的无线通信模块进行交易，记录实体银行卡的交易位置和交易时间，分别作为第四交易位置和第四交易时间，第四交易位置和第四交易时间形成第四交易日志。请参考步骤110。

[0060] 步骤119：银行后台对第四交易日志进行认证，请参考步骤111。

[0061] 步骤120:判断第四交易日志的认证是否通过。

[0062] 若第四交易日志的认证通过,则执行步骤121:银行后台执行解锁指令。

[0063] 若第一交易位置属于银行卡预设的交易城市列表,并且该交易不是银行卡持卡人所认可的交易,则属于本地盗刷,银行卡持卡人发生了经济损失,需要登录银行后台及时锁卡。具体包括如下步骤:

[0064] 步骤103:判断银行后台是否接收到锁卡指令。

[0065] 若银行后台接收到锁卡指令,则执行步骤104:银行后台利用实体银行卡通过移动终端的无线通信模块(如NFC模块)进行交易,记录实体银行卡的交易位置和交易时间,分别作为第三交易位置和第三交易时间,第三交易位置和第三交易时间形成第三交易日志。请参见步骤110。

[0066] 步骤105:银行后台对第三交易日志进行认证,请参见步骤111。

[0067] 步骤106:判断第三交易日志的认证是否通过。

[0068] 若第三交易日志认证通过,则执行步骤107:银行后台执行锁卡指令,实现一键锁卡。

[0069] 锁卡后用户可通过银行后台进行解锁,请参考步骤117-步骤120。

[0070] 本申请使用银行后台进行卡片身份验证,记录交易日志,证明银行卡在身边,同时可以通过锁卡功能,直接将银行卡锁定。该方法不受空间影响,只需有支持NFC等近场无线通信功能及GPS功能的手机,GPS地理信息不会被篡改,可以被银行所接受;不受时间限制,可及时进行卡片认证,由于认证及时,地理信息的及时上报,盗刷现象很容易被银行认可;操作简单,节省时间,并且一键锁卡功能可以更快的避免损失;无需对银行卡进行任何结构改变,适用于现有的银行卡。

[0071] 本申请利用移动终端的NFC、蓝牙或wifi等近场无线通信对实体银行卡进行操作获取凭证,并通过移动终端上的微信公众号或银行客户端对银行卡进行锁卡操作,避免用户通过电话或柜台证明银行卡和用户不在交易所在地导致的延迟和损失。

[0072] 实施例二

[0073] 本申请还提供了与上述方法相应的移动终端。图2为本申请实施例提供的移动终端的结构图。如图2所示,移动终端包括第一交易日志接收模块210,用于接收银行发送的银行卡的第一交易日志,第一交易日志包括第一交易位置和第一交易时间。该第一交易日志可以通过短信接收,也可以通过微信公众号或银行客户端接收,使得用户获知该交易正在发生。

[0074] 移动终端包括银行卡所属的银行的银行后台220。如图3所示,银行后台包括用户指令接收模块2201、实体卡交易模块2202、第二交易日志认证模块2203、指令执行模块2204、自动锁卡模块2205以及自动解锁模块2206。

[0075] 用户指令接收模块2201用于接收用户输入的指令。

[0076] 实体卡交易模块2202与用户指令接收模块2201连接,用于利用实体银行卡通过移动终端的无线通信模块进行交易,记录实体银行卡的交易位置和交易时间,分别作为第二交易位置和第二交易时间,第二交易位置和第二交易时间形成第二交易日志。

[0077] 第二交易日志认证模块2203与实体卡交易模块2202连接,用于对第二交易日志进行认证。

[0078] 指令执行模块2204与第二交易日志认证模块2203连接，用于响应于第二交易日志的认证通过而执行用户输入的指令。

[0079] 自动锁卡模块2205，用于响应于第一交易位置不属于银行卡预设的交易城市列表，并且银行卡连续被使用指定次数并且该指定次数中每次都未接收到用户的锁卡指令而执行自动锁卡。

[0080] 自动解锁模块2206与自动锁卡模块2205连接，用于自自动锁卡起指定时间后自动对银行卡进行解锁。

[0081] 如图4所示，实体卡交易模块2202包括APDU指令发送模块22021和交易数据接收模块22022。

[0082] APDU指令发送模块22021用于通过无线通信模块向实体银行卡发送APDU指令，APDU指令为交易金额为0的GPO认证。

[0083] 交易数据接收模块22022用于通过无线通信模块接收实体银行卡返回的对APDU指令的交易数据。

[0084] 如图5所示，第二交易日志认证模块2203包括交易数据接收模块22031、加密数据获取模块22032、格式验证模块22033、哈希值计算模块22034以及数据判断模块22035；

[0085] 交易数据接收模块22031，用于通过无线通信模块接收交易数据；

[0086] 加密数据获取模块22032与交易数据接收模块22031连接，用于使用公钥和指数对脱机交易产生的交易数据进行加密，获得加密数据；

[0087] 格式验证模块22033与加密数据获取模块22032连接，用于验证加密数据是否符合正确的数据格式；

[0088] 哈希值计算模块22034与格式验证模块22033和加密数据获取模块22032连接，用于响应于格式验证通过而获取加密数据中的部分数据，并利用部分数据和银行客户端产生的随机数计算哈希值；

[0089] 数据判断模块22035与哈希值计算模块22034连接，用于判断哈希值与加密数据是否相同。

[0090] 本申请利用移动终端的NFC、蓝牙或wifi等近场无线通信对实体银行卡进行操作获取凭证，快速而方便的证明真卡与伪卡的非同一性，并通过移动终端上的微信公众号或银行客户端对银行卡进行锁卡操作，避免用户通过电话或柜台证明银行卡和用户不在交易所在地导致的延迟和损失。

[0091] 尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

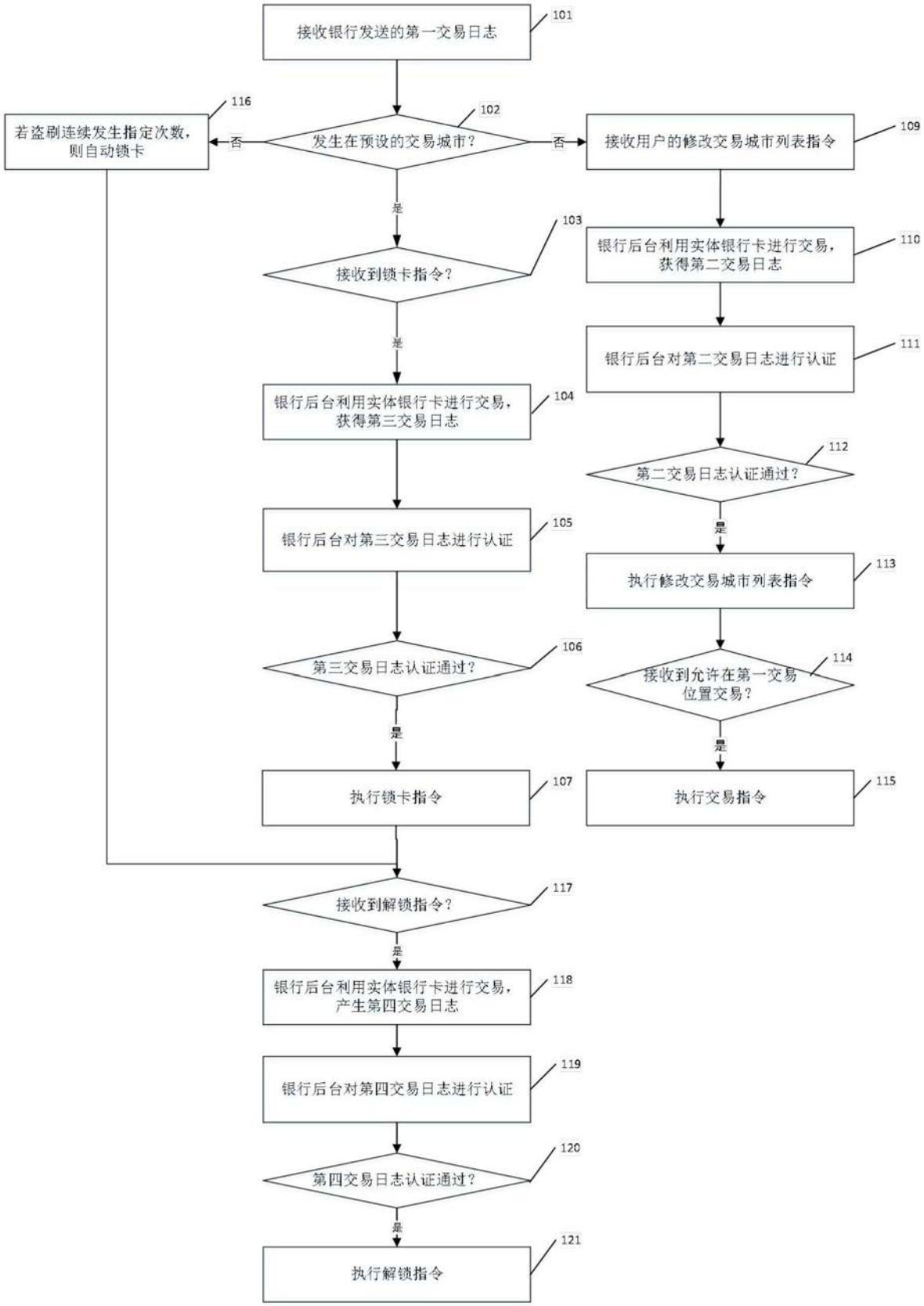

接收银行发送的第一交易日志
101
发生在预设的交易城市?
102
否
若盗刷连续发生指定次数，则自动锁卡
116
否
接收用户的修改交易城市列表指令
109
是
接收到锁卡指令?
103
是
银行后台利用实体银行卡进行交易，获得第三交易日志
104
银行后台对第三交易日志进行认证
105
第三交易日志认证通过?
106
是
执行锁卡指令
107
银行后台利用实体银行卡进行交易，获得第二交易日志
110
银行后台对第二交易日志进行认证
111
第二交易日志认证通过?
112
是
执行修改交易城市列表指令
113
接收到允许在第一交易位置交易?
114
是
执行交易指令
115
接收到解锁指令?
117
是
银行后台利用实体银行卡进行交易，产生第四交易日志
118
银行后台对第四交易日志进行认证
119
第四交易日志认证通过?
120
是
执行解锁指令
121

图1

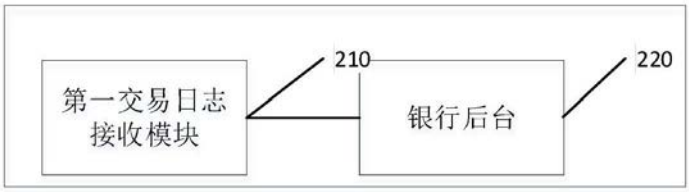

第一交易日志接收模块
210
银行后台
220

图2

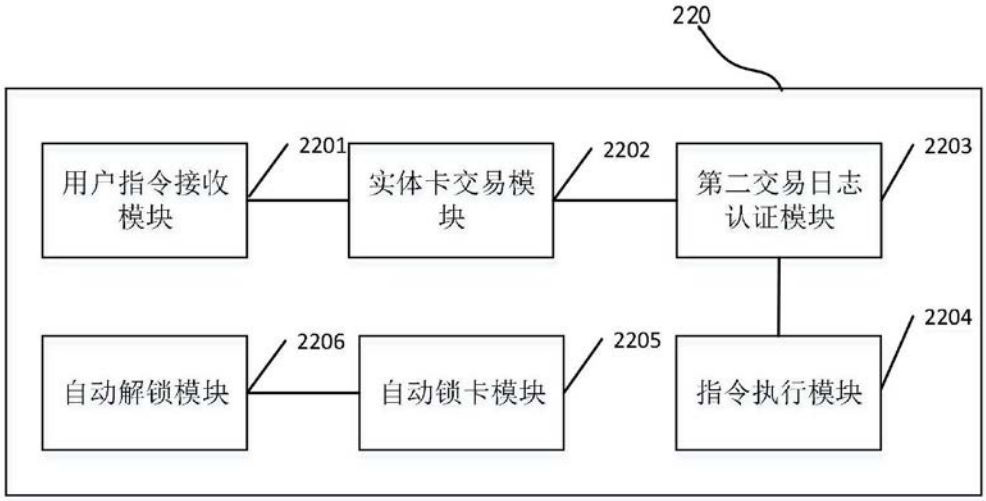

220
用户指令接收模块
2201
实体卡交易模块
2202
第二交易日志认证模块
2203
自动解锁模块
2206
自动锁卡模块
2205
指令执行模块
2204

图3

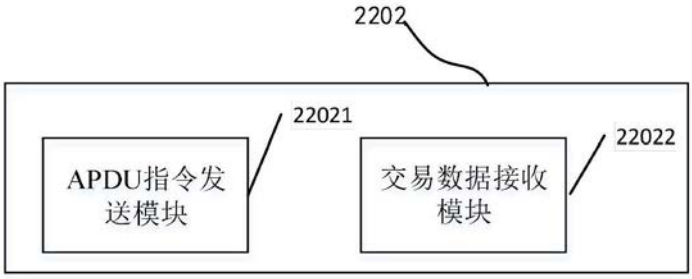

2202
APDU指令发送模块
22021
交易数据接收模块
22022

图4

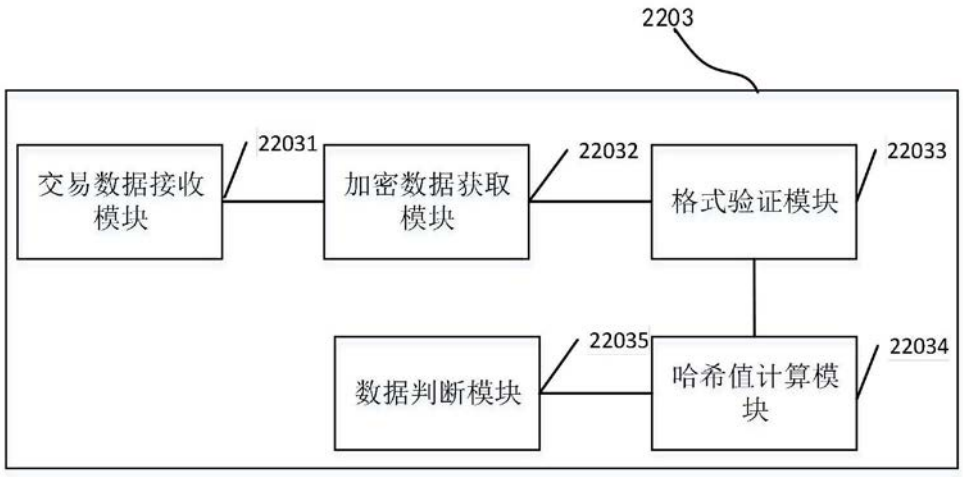

2203
交易数据接收模块
22031
加密数据获取模块
22032
格式验证模块
22033
数据判断模块
22035
哈希值计算模块
22034

图5