



(12)发明专利

(10)授权公告号 CN 106980981 B

(45)授权公告日 2020.01.31

(21)申请号 201710216858.5

CN 102611943 A,2012.07.25,

(22)申请日 2017.04.05

US 2011/0240745 A1,2011.10.06,

(65)同一申请的已公布的文献号

审查员 孙凤

申请公布号 CN 106980981 A

(43)申请公布日 2017.07.25

(73)专利权人 恒宝股份有限公司

地址 212355 江苏省镇江市横塘工业区

(72)发明人 高岚 陆道如

(51)Int.Cl.

G06Q 20/38(2012.01)

G06Q 20/40(2012.01)

G06Q 20/34(2012.01)

(56)对比文件

CN 104318436 A,2015.01.28,

CN 103679444 A,2014.03.26,

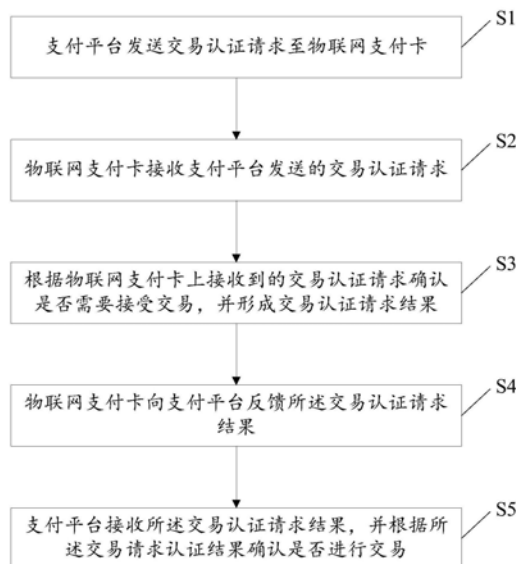
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种物联网支付卡的线上有卡支付方法及其支付系统

(57)摘要

本发明公开了一种物联网支付卡的线上有卡支付方法及其支付系统,其中,物联网支付卡的线上有卡支付方法包括步骤S1:支付平台发送交易认证请求至物联网支付卡;步骤S2:物联网支付卡接收支付平台发送的交易认证请求;步骤S3:根据物联网支付卡上接收到的交易认证请求确认是否需要接受交易,并形成交易认证请求结果;步骤S4:物联网支付卡向支付平台反馈所述交易认证请求结果;步骤S5:支付平台接收所述交易认证请求结果,并根据所述交易请求认证结果确认是否进行交易。本发明中,需要物联网支付卡参与线上支付过程中,而物联网支付卡自身具有高级别的安全防伪认证功能,因此提高了用户账户的安全,避免了银行卡在手中,卡中资金却被盗的情况发生。



CN 106980981 B

1. 一种物联网支付卡的线上有卡支付方法,其特征在于,包括:

步骤S1:支付平台发送交易认证请求至物联网支付卡;

步骤S2:物联网支付卡接收支付平台发送的交易认证请求;

步骤S3:根据物联网支付卡上接收到的交易认证请求确认是否需要接受交易,通过物联网支付卡的显示屏显示该交易认证请求进行核对,核对后,通过物联网支付卡的交易按键确认是否继续进行交易;确认继续进行交易后,运用物联网支付卡自身的安全防伪功能运算生成交易认证请求结果;

步骤S4:物联网支付卡向支付平台反馈所述交易认证请求结果;

步骤S5:支付平台接收所述交易认证请求结果,并根据所述交易请求认证结果确认是否进行交易。

2. 根据权利要求1所述的物联网支付卡的线上有卡支付方法,其特征在于,在步骤S1之前还包括:

步骤S01:从互联网设备上的互联网购物商城选购商品,并向支付平台发起支付订单请求;

步骤S02:支付平台接收所述支付订单请求,并向互联网设备反馈交易认证请求;

步骤S03:互联网设备接收并向用户展示所述交易认证请求;

步骤S04:用户根据互联网设备展示的所述交易认证请求,在互联网设备中输入物联网支付卡的相关信息;

步骤S05:互联网设备向支付平台发送物联网支付卡的相关信息;

步骤S06:支付平台接收到物联网设备发送的物联网支付卡的相关信息,并与该物联网支付卡建立基于物联网通信的无线连接。

3. 根据权利要求2所述的物联网支付卡的线上有卡支付方法,其特征在于,步骤S06具体包括:

步骤S061:物联网支付卡向物联网基站发送包含该物联网支付卡信息的入网信息;

步骤S062:物联网基站接收所述入网信息,并发送所述入网信息至物联网设备管理平台;

步骤S063:所述物联网设备管理平台接收所述入网信息,并将所述入网信息发送至所述支付平台;

步骤S064:所述支付平台接收所述入网信息;

步骤S065:支付平台接收物联网设备发送的物联网支付卡的相关信息,与接收到的所述入网信息相匹配,并与匹配成功的所述入网信息对应的物联网支付卡之间建立通信连接。

4. 根据权利要求1所述的物联网支付卡的线上有卡支付方法,其特征在于,步骤S1具体包括:

步骤S11:支付平台向物联网设备管理平台发送交易认证请求;

步骤S12:物联网设备管理平台接收交易认证请求并向物联网基站发送交易认证请求;

步骤S13:物联网基站接收交易认证请求,并向物联网支付卡发送交易认证请求。

5. 根据权利要求1所述的物联网支付卡的线上有卡支付方法,其特征在于,步骤S4具体包括:

步骤S41:物联网支付卡将交易认证请求结果发送至物联网基站;

步骤S42:物联网基站接收交易认证请求结果,并发送至物联网设备管理平台;

步骤S43:物联网设备管理平台接收交易认证结果,并发送至支付平台。

6.一种物联网支付卡的线上有卡支付系统,其特征在于,包括:

支付平台,所述支付平台用于发送交易认证请求,并接收交易认证请求结果,确认是否进行交易;

物联网支付卡,所述物联网支付卡用于接收所述支付平台发送的交易认证请求,对交易认证请求进行确认,通过物联网支付卡的显示屏显示该交易认证请求进行核对,核对后,通过物联网支付卡的交易按键确认是否继续进行交易;确认继续进行交易后,运用物联网支付卡自身的安全防伪功能运算生成;并运用物联网支付卡自身的安全防伪功能运算生成交易认证请求结果,将所述交易认证请求结果反馈至所述支付平台。

7.根据权利要求6所述的物联网支付卡的线上有卡支付系统,其特征在于,所述物联网支付卡包括集成于卡片内部的物联网天线,通过所述物联网天线与支付平台通信。

8.根据权利要求6所述的物联网支付卡的线上有卡支付系统,其特征在于,还包括:

互联网设备,用户从互联网设备上的互联网购物商城选购商品,并向支付平台发起支付订单请求;

支付平台接收所述支付订单请求,并向互联网设备反馈交易认证请求;

互联网设备接收并向用户展示所述交易认证请求;

用户根据互联网设备展示的所述交易认证请求,在互联网设备中输入物联网支付卡的相关信息;

互联网设备向支付平台发送物联网支付卡的相关信息;

支付平台接收到物联网设备发送的物联网支付卡的相关信息,并与该物联网支付卡建立基于物联网通信的无线连接。

9.根据权利要求8所述的物联网支付卡的线上有卡支付系统,其特征在于,物联网支付卡向物联网基站发送包含该物联网支付卡信息的入网信息;

物联网基站接收所述入网信息,并发送所述入网信息至物联网设备管理平台;

所述物联网设备管理平台接收所述入网信息,并将所述入网信息发送至所述支付平台;

所述支付平台接收所述入网信息;

所述支付平台接收物联网设备发送的物联网支付卡的相关信息,与接收到的所述入网信息相匹配,并与匹配成功的所述入网信息对应的物联网支付卡之间建立通信连接。

10.根据权利要求8所述的物联网支付卡的线上有卡支付系统,其特征在于,所述支付平台发送交易认证请求至物联网支付卡具体包括:

支付平台通过物联网设备管理平台、物联网基站向物联网支付卡发送交易认证请求。

## 一种物联网支付卡的线上有卡支付方法及其支付系统

### 技术领域

[0001] 本发明涉及银行卡的支付技术领域,尤其涉及一种物联网支付卡的线上有卡支付方法及其支付系统。

### 背景技术

[0002] 目前银行卡的线上支付的流程是,先将银行卡绑定支付宝或微信等支付平台,在需要进行支付时,仅需要输入支付宝或微信的密码即可。而实体卡在整个线上支付过程中,仅参与与支付宝或微信等支付平台绑定这一过程,在后续的使用过程中,完全抛弃了实体卡自身的安全性能,仅依靠支付宝或微信等支付平台的安全性来保证,而当用户的支付宝或微信等含有支付功能的平台被攻击突破时,往往会伴随着用户银行卡中的资金被盗的情况出现。如此全舍弃银行卡自身具有的安全防伪认证功能,必然会降低用户账户的安全保障,而在日常生活中,也常常会出现银行卡在用户的手中,卡中的资金却被盗刷的情况,给用户的财产带来极大的损失。

### 发明内容

[0003] 本发明的目的在于提供一种物联网支付卡的线上有卡支付方法及系统,用于避免出现银行卡在用户手中,卡中资金却被盗刷的情况出现。

[0004] 为达到上述目的,本发明提供的物联网支付卡的线上有卡支付方法及系统采用如下技术方案:

[0005] 一种物联网支付卡的线上有卡支付方法,包括:

[0006] 步骤S1:支付平台发送交易认证请求至物联网支付卡;

[0007] 步骤S2:物联网支付卡接收支付平台发送的交易认证请求;

[0008] 步骤S3:根据物联网支付卡上接收到的交易认证请求确认是否需要接受交易,并形成交易认证请求结果;

[0009] 步骤S4:物联网支付卡向支付平台反馈所述交易认证请求结果;

[0010] 步骤S5:支付平台接收所述交易认证请求结果,并根据所述交易请求认证结果确认是否进行交易。

[0011] 如上所述的物联网支付卡的线上有卡支付方法,其中,优选的是,在步骤S1之前还包括:

[0012] 步骤S01:从互联网设备上的互联网购物商城选购商品,并向支付平台发起支付订单请求;

[0013] 步骤S02:支付平台接收所述支付订单请求,并向互联网设备反馈交易认证请求;

[0014] 步骤S03:互联网设备接收并向用户展示所述交易认证请求;

[0015] 步骤S04:用户根据互联网设备展示的所述交易认证请求,在互联网设备中输入物联网支付卡的相关信息;

[0016] 步骤S05:互联网设备向支付平台发送物联网支付卡的相关信息;

[0017] 步骤S06:支付平台接收到物联网设备发送的物联网支付卡的相关信息,并与该物联网支付卡建立基于物联网通信的无线连接。

[0018] 如上所述的物联网支付卡的线上有卡支付方法,其中,优选的是,步骤S06具体包括:

[0019] 步骤S061:物联网支付卡向物联网基站发送包含该物联网支付卡信息的入网信息;

[0020] 步骤S062:物联网基站接收所述入网信息,并发送所述入网信息至物联网设备管理平台;

[0021] 步骤S063:所述物联网设备管理平台接收所述入网信息,并将所述入网信息发送至所述支付平台;

[0022] 步骤S064:所述支付平台接收所述入网信息;

[0023] 步骤S065:支付平台接收物联网设备发送的物联网支付卡的相关信息,与接收到的所述入网信息相匹配,并与匹配成功的所述入网信息对应的物联网支付卡之间建立通信连接。

[0024] 如上所述的物联网支付卡的线上有卡支付方法,其中,优选的是,步骤S1具体包括:

[0025] 步骤S11:支付平台向物联网设备管理平台发送交易认证请求;

[0026] 步骤S12:物联网设备管理平台接收交易认证请求并向物联网基站发送交易认证请求;

[0027] 步骤S13:物联网基站接收交易认证请求,并向物联网支付卡发送交易认证请求。

[0028] 如上所述的物联网支付卡的线上有卡支付方法,其中,优选的是,步骤S4具体包括:

[0029] 步骤S41:物联网支付卡将交易认证请求结果发送至物联网基站;

[0030] 步骤S42:物联网基站接收交易认证请求结果,并发送至物联网设备管理平台;

[0031] 步骤S43:物联网设备管理平台接收交易认证结果,并发送至支付平台。

[0032] 一种物联网支付卡的线上有卡支付系统,包括:

[0033] 支付平台,所述支付平台用于发送交易认证请求,并接收交易认证请求结果,确认是否进行交易;

[0034] 物联网支付卡,所述物联网支付卡用于接收所述支付平台发送的交易认证请求,并对交易认证请求进行确认形成交易认证请求结果,将所述交易认证请求结果反馈至所述支付平台。

[0035] 如上所述的物联网支付卡的线上有卡支付系统,其中,优选的是,所述物联网支付卡包括集成于卡片内部的物联网天线,通过所述物联网天线与支付平台通信。

[0036] 如上所述的物联网支付卡的线上有卡支付系统,其中,优选的是,还包括:

[0037] 互联网设备,用户从互联网设备上的互联网购物商城选购商品,并向支付平台发起支付订单请求;

[0038] 支付平台接收所述支付订单请求,并向互联网设备反馈交易认证请求;

[0039] 互联网设备接收并向用户展示所述交易认证请求;

[0040] 用户根据互联网设备展示的所述交易认证请求,在互联网设备中输入物联网支付



明中的实施例,本领域普通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,都属于本发明保护的范围。

#### [0059] 实施例一

[0060] 本发明实施例提供一种物联网支付卡的线上有卡支付方法的支付系统如图1-图2所示,该支付系统包括互联网设备、物联网设备管理平台、物联网基站、支付平台和物联网支付卡。互联网设备可为各种计算设备,例如手机、PAD等移动终端或电脑等。物联网设备管理平台和支付平台可为计算设备或计算设备上运行的软件。物联网基站和物联网支付卡基于物联网实现通信,其中物联网支付卡的构造如图2所示,包括:集成于卡片1内部的物联网络天线2、物联网通信芯片3、主控芯片4、安全存储芯片5和交易按键6,其中使用物联网络天线2和物联网通信芯片3组成的物联网通信装置实现物联网支付卡与支付平台之间进行基于物联网的数据交互,主控芯片4通过物联网通信装置接收和发送外部数据,安全存储芯片5储存有物联网支付卡自身的安全认证信息,并根据用户的选择通过自身的运算对外部信息进行安全认证,交易按键6用于给用户对交易进行确认。

[0061] 本实施例中,用户从互联网设备的购物商城中选购商品,在支付平台中形成订单支付请求,同时支付平台向物联网支付卡发送交易认证请求,用户通过操作物联网支付卡中的交易按键6确定是否同意交易,安全存储芯片5根据用户的选择通过自身的运算形成交易认证请求结果,并通过主控芯片4反馈至支付平台,支付平台根据接收到的交易认证请求结果最终确定是否进行交易。

[0062] 其中物联网支付卡与支付平台之间的通信是通过物联网完成的,具体地,支付平台将需要交互的数据发送至物联网设备管理平台,物联网设备管理平台接收需要交互的数据并发送至物联网基站,物联网基站最终将需要交互的数据发送至物联网支付卡,由于物联网支付卡内部集成有物联网络天线2和物联网通信芯片3,因此物联网支付卡可以基于物联网收发信息并进行数据交互,再经过用户的确认后通过物联网基站和物联网设备管理平台反馈至支付平台,支付平台最终根据物联网支付卡反馈的数据确认是否进行交易。在此交易过程中,需要用户通过在实体卡上的操作才能最终完成交易,这样一来,在线上支付的过程中,也需要用到实体卡自身的防伪认证功能,从而增加用户资金的安全保障,防止银行卡在身上,卡中资金却被盗的情况出现。

#### [0063] 实施例二

[0064] 下面介绍上述物联网支付系统的工作方法,即本物联网支付卡的线上有卡支付方法,该物联网支付卡的线上有卡支付方法具体包括如下步骤:

[0065] 步骤S01:从互联网设备上的互联网购物商城选购商品,并向支付平台发起支付订单请求。互联网设备与支付平台之间是通过互联网进行信息传递的。本领域技术人员可以理解的是,支付平台可以是支持支付宝和微信的具有支付功能的第三方支付平台或银行自身的支付平台。

[0066] 步骤S02:支付平台接收所述支付订单请求,并向互联网设备反馈交易认证请求。

[0067] 步骤S03:互联网设备接收并向用户展示所述交易认证请求。

[0068] 通过以上三个步骤,将用户选购的商品形成交易认证请求,在传统的支付过程中,此时仅需输入支付平台的交易密码即可完成交易,显然,在传统的网上交易过程中无需实体银行卡参与,而完全抛弃了实体银行卡自身的防伪认证功能,从而降低了用户账户的安

全性能。

[0069] 步骤S04:用户根据互联网设备展示的所述交易认证请求,在互联网设备中输入物联网支付卡的相关信息。具体地,物联网支付卡的相关信息包括卡号、安全码和有效期等能表征该物联网支付卡的信息。本领域技术人员可以理解的是,物联网支付卡的相关信息可以保存在支付平台中,等下次需要使用时能直接调出,从而可以节省用户的时间。

[0070] 步骤S05:互联网设备向支付平台发送物联网支付卡的相关信息。

[0071] 步骤S06:支付平台接收到物联网设备发送的物联网支付卡的相关信息,并与该物联网支付卡建立基于物联网通信的无线连接。

[0072] 具体地,需打开物联网支付卡的电源开关,使得物联网支付卡处于联网状态。物联网支付卡向物联网基站发送包含该物联网支付卡信息的入网信息,该入网信息中包含有物联网支付卡的卡号、安全码和有效期等能表征该物联网支付卡特征的相关信息。物联网基站接收到入网信息后,再将入网信息发送至物联网设备管理平台,物联网设备管理平台接收到该入网信息后再发送至支付平台。支付平台接收到该包含有物联网支付卡特征的入网信息和物联网设备发送的物联网支付卡的相关信息,并将二者的信息相匹配,当匹配成功时,便建立起与该物联网支付卡之间的基于物联网的通信连接,即支付平台与物联网支付卡之间建立起信息交互通道,如此建立起的交互通道能保证准确性和单一性。如此一来,支付平台就能准确的将交易认证请求发送至用户的物联网支付卡。

[0073] 如图3所示,物联网支付的线上有卡支付方法,包括:步骤S1:支付平台发送交易认证请求至物联网支付卡。

[0074] 具体地,支付平台向物联网设备管理平台发送交易认证请求,物联网设备管理平台接收交易认证请求并向物联网基站发送交易认证请求,物联网基站接收交易认证请求,并向物联网支付卡发送交易认证请求。从而,支付平台完成通过物联网向物联网支付卡发送交易认证请求的过程。

[0075] 步骤S2:物联网支付卡接收支付平台发送的交易认证请求。

[0076] 步骤S3:根据物联网支付卡上接收到的交易认证请求确认是否需要接受交易,并形成交易认证请求结果。

[0077] 具体地,用户需要操作物联网支付卡,最终确认交易信息是否正确,并决定是否接收交易,同时物联网支付卡根据用户的选择或输入运用自身的安全防伪功能运算生成交易认证请求结果。本领域技术人员可以理解的是,物联网支付卡中还包括可以显示交易信息的显示屏,该显示屏中可以显示交易金额等相关信息,用户可以核对交易金额等相关的交易信息,以确保本次交易的准确性。同时,该物联网支付卡中还设置有确认或取消交易的交易按键,用于给用户选择是否进行交易。在此过程中,物联网支付卡参与到了线上支付的过程,从而可以使用到物联网支付卡自身的防伪认证功能,提高了用户账户的安全保障。

[0078] 步骤S4:物联网支付卡向支付平台反馈所述交易认证请求结果。

[0079] 具体地,物联网支付卡将交易认证请求结果发送至物联网基站;物联网基站接收交易认证请求结果,并发送至物联网设备管理平台;物联网设备管理平台接收交易认证结果,并发送至支付平台。

[0080] 步骤S5:支付平台接收所述交易认证请求结果,并根据所述交易请求认证结果确认是否进行交易。

[0081] 具体地,支付平台判定交易请求认证结果是否正确,若是,则进行交易并将完成交易信息展示在互联网设备上;若否,则将错误信息展示在互联网设备上。本领域技术人员可以理解的是,当判定交易请求结果正确时,进行交易即表示用户从互联网商城上完成购物,当判定交易请求结果不正确时,用户可以根据互联网设备展示错误提示进行修改或直接结束本次交易。

[0082] 本实施例中,用户在使用物联网支付卡进行线上支付时,与传统银行卡的线上支付相比较,最大的不同是需要物联网支付卡参与到整个支付过程中,而又由于银行卡在出厂时设置了自身的安全防伪认证功能,且为了保证用户的账户的安全,此安全防伪认证功能的安全级别很高,因此在传统的银行卡的线上支付过程中,舍弃银行卡自身的安全防伪认证功能,相当于极大程度上的降低了用户账户的安全级别。而本实施例中的物联网支付卡自身需要参与到线上支付的过程中,从而可以使用到自身的安全防伪认证功能,从而提高了用户账户的安全级别,避免出现银行卡在身上,卡中的资金却被盗刷的情况。

[0083] 以上所述,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以所述权利要求的保护范围为准。

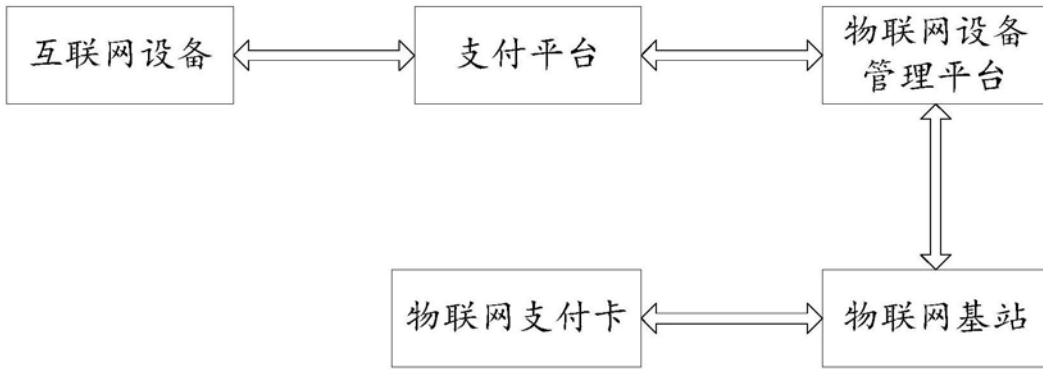


图1

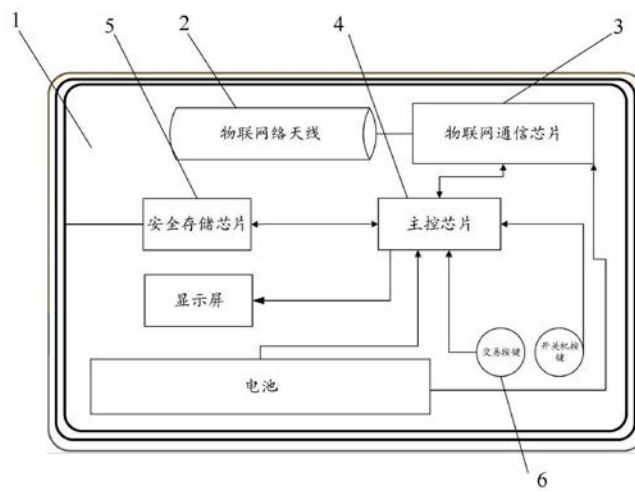


图2

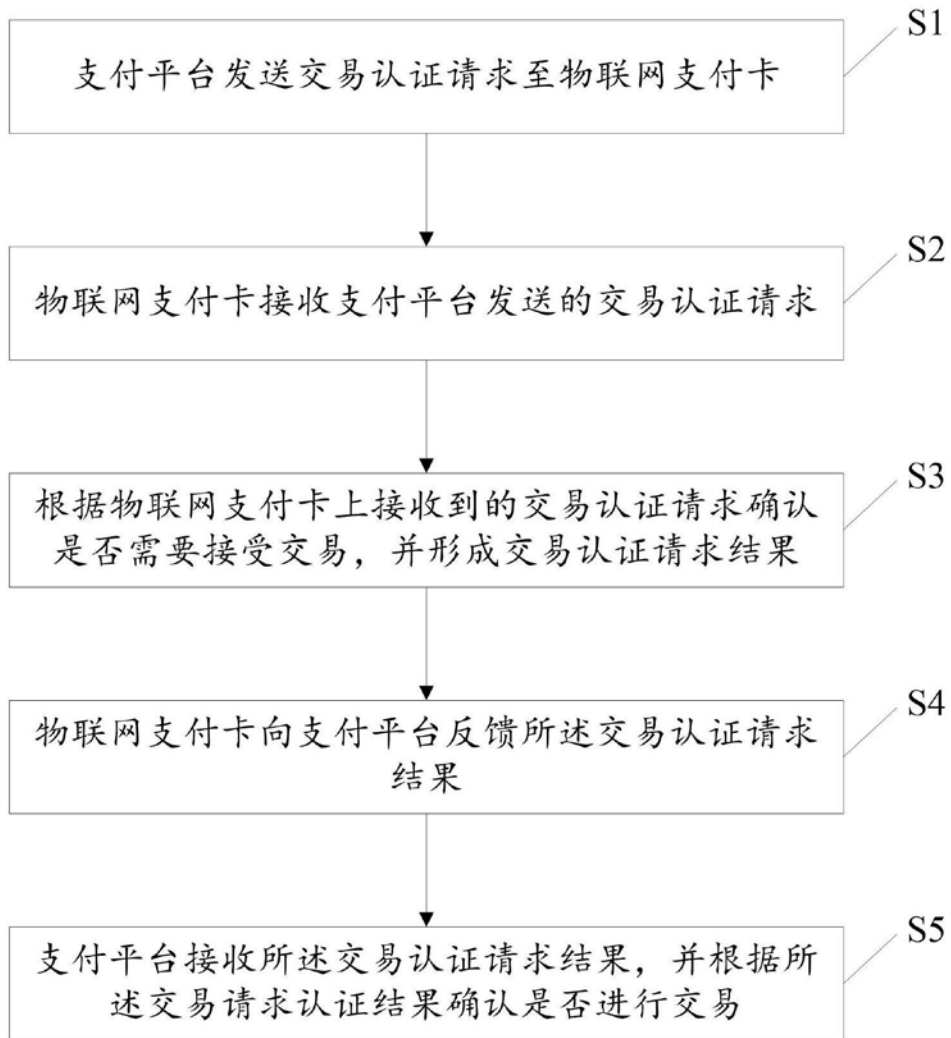


图3