(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113159744 A
(43)申请公布日 2021.07.23

(21)申请号 202110175166.7
(22)申请日 2021.02.07
(71)申请人 思特沃克软件技术(武汉)有限公司
地址 430000 湖北省武汉市东湖新技术开发区关山大道332号保利国际中心20层
(72)发明人 鄢倩 刘尚奇 沈寅 张诚 王智慧
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 尹秀
(51)Int.Cl.
G06Q 20/06(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
G06Q 20/42(2012.01)

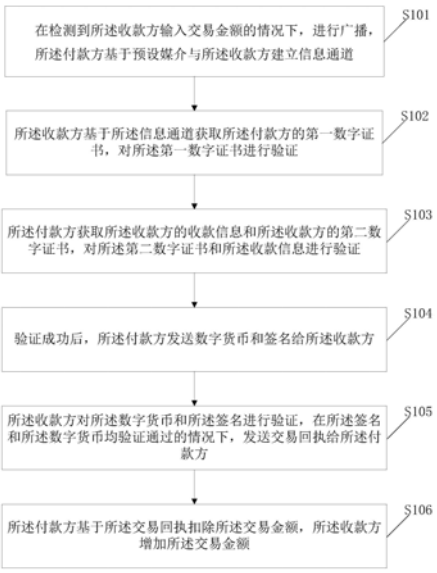
权利要求书2页 说明书9页 附图4页

(54)发明名称

一种数字货币的双离线支付系统、方法及装置

(57)摘要

本发明公开了一种数字货币的双离线支付系统，应用于收款方和付款方，付款方和收款方组成区块链，所述系统包括：在检测到收款方输入交易金额的情况下，进行广播，付款方基于预设媒介与收款方建立信息通道；收款方基于信息通道获取付款方的第一数字证书并进行验证；付款方获取收款方的收款信息和收款方的第二数字证书并进行验证；验证成功后，付款方发送数字货币和签名给收款方令收款方进行验证，在签名和数字货币均验证通过的情况下，发送交易回执给付款方；付款方基于交易回执扣除交易金额，收款方增加交易金额。上述过程，实现了在没有网络条件下，基于预设媒介建立信息通道，基于信息通道实现收款方和付款方的离线支付，不受网络环境限制。



CN 113159744 A

1.一种数字货币的双离线支付系统,其特征在于,应用于收款方和付款方,所述付款方和所述收款方组成区块链,所述系统包括:

在检测到所述收款方输入交易金额的情况下,进行广播,所述付款方基于预设媒介与所述收款方建立信息通道;

所述收款方基于所述信息通道获取所述付款方的第一数字证书,对所述第一数字证书进行验证;

所述付款方获取所述收款方的收款信息和所述收款方的第二数字证书,对所述第二数字证书和所述收款信息进行验证;

验证成功后,所述付款方发送数字货币和签名给所述收款方;

所述收款方对所述数字货币和所述签名进行验证,在所述签名和所述数字货币均验证通过的情况下,发送交易回执给所述付款方;

所述付款方基于所述交易回执扣除所述交易金额,所述收款方增加所述交易金额。

2.根据权利要求1所述的系统,其特征在于,所述区块链还包括:银行区块链系统,

在检测到所述区块链处于有网络情况下时,获取所述付款方和所述收款方的交易信息;

所述银行区块链系统基于所述交易信息对所述收款方、所述付款方和所述交易金额进行验证;

在验证通过的情况下,更改所述付款方和所述收款方的交易状态。

3.根据权利要求1所述的系统,其特征在于,所述付款方基于预设媒介与所述收款方建立信息通道,包括:

所述付款方询问所述收款方的随机公钥;

所述收款方将所述随机公钥发送给所述付款方进行应答;

所述付款方基于所述随机公钥加密随机密钥发送给收款方;

所述收款方基于所述随机密钥加密回复确认应答。

4.根据权利要求1所述的系统,其特征在于,对所述第二数字证书和所述收款信息进行验证,包括:

对所述收款方进行验证;

获取所述收款信息中的交易金额,对所述交易金额进行验证;

基于根证书验证所述第二数字证书。

5.根据权利要求1所述的系统,其特征在于,所述交易回执包括:所述付款方、所述交易金额、所述收款方和所述交易标识,若所述付款方为收到所述交易回执,将所述信息通道断开,基于所述预设媒介重新建立所述付款方和所述收款方的信息通道。

6.根据权利要求1所述的系统,其特征在于,所述收款方中所述交易金额的交易状态为临时状态。

7.一种数字货币的双离线支付方法,其特征在于,应用于收款方,所述方法包括:

在检测到所述收款方输入交易金额的情况下,进行广播,以令付款方与所述收款方建立信息通道;

基于所述信息通道获取所述付款方的第一数字证书,对所述第一数字证书进行验证;

验证通过后,接收所述付款方发送的数字货币和签名,对所述数字货币和所述签名进

行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方。

8.一种数字货币的双离线支付方法，其特征在于，应用于付款方，所述方法包括：

在接收到收款方广播的情况下，所述付款方基于预设媒介与所述收款方建立信息通道；

在接收到所述收款方对所述付款方验证通过指令的情况下，获取所述收款方的收款信息和所述收款方的第二数字证书，对所述第二数字证书和所述收款信息进行验证；

验证成功后，发送数字货币和签名给所述收款方，以令所述收款方对所述数字货币和所述签名进行验证，验证通过的情况下，发送交易回执；

接收所述交易回执，基于所述交易回执扣除对应交易金额。

9.一种数字货币的双离线支付装置，其特征在于，应用于收款方，所述装置包括：

广播模块，用于在检测到所述收款方输入交易金额的情况下，进行广播，以令付款方与所述收款方建立信息通道；

验证模块，用于基于所述信息通道获取所述付款方的第一数字证书，对所述第一数字证书进行验证；

验证和发送模块，用于验证通过后，接收所述付款方发送的数字货币和签名，对所述数字货币和所述签名进行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方。

10.一种数字货币的双离线支付装置，其特征在于，应用于付款方，所述装置包括：

建立模块，用于在接收到收款方广播的情况下，所述付款方基于预设媒介与所述收款方建立信息通道；

获取和验证模块，用于在接收到所述收款方对所述付款方验证通过指令的情况下，获取所述收款方的收款信息和所述收款方的第二数字证书，对所述第二数字证书和所述收款信息进行验证；

发送模块，用于验证成功后，发送数字货币和签名给所述收款方，以令所述收款方对所述数字货币和所述签名进行验证，验证通过的情况下，发送交易回执；

扣除模块，用于接收所述交易回执，基于所述交易回执扣除对应交易金额。

一种数字货币的双离线支付系统、方法及装置

技术领域

[0001] 本发明涉及互联网技术领域，尤其涉及一种数字货币的双离线支付系统、方法及装置。

背景技术

[0002] 数字货币或将采用“一币两库三中心”架构，两库指的是央行发行库和商业银行的银行库，三中心包括认证中心、登记中心和大数据分析中心。这其中，认证中心负责央行数字货币机构及用户的真实身份信息采集等管理工作。登记中心负责记录数字货币和用户钱包记录，完成权属登记，同时记录数字货币发行、转移、回笼全过程信息。大数据分析中心旨在运用大数据分析DCEP的发行、流通、贮藏等，具有反洗钱、支付行为分析、监管调控指标分析等功能。

[0003] 数字货币作为电子货币的一种，在交易双方基于数字货币进行交易时，需要基于网络下可以实现付款方向收款方进行支付，在无网络条件应进行支付收到限制。

发明内容

[0004] 有鉴于此，本发明提供了一种数字货币的双离线支付系统、方法及装置，用以解决在交易双方基于数字货币进行交易时，需要基于网络下可以实现付款方向收款方进行支付，在无网络条件应进行支付收到限制的问题。具体方案如下：

一种数字货币的双离线支付系统，应用于收款方和付款方，所述付款方和所述收款方组成区块链，所述系统包括：

在检测到所述收款方输入交易金额的情况下，进行广播，所述付款方基于预设媒介与所述收款方建立信息通道；

所述收款方基于所述信息通道获取所述付款方的第一数字证书，对所述第一数字证书进行验证；

所述付款方获取所述收款方的收款信息和所述收款方的第二数字证书，对所述第二数字证书和所述收款信息进行验证；

验证成功后，所述付款方发送数字货币和签名给所述收款方；

所述收款方对所述数字货币和所述签名进行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方；

所述付款方基于所述交易回执扣除所述交易金额，所述收款方增加所述交易金额。

[0005] 上述的系统，可选的，所述区块链还包括：银行区块链系统，

在检测到所述区块链处于有网络情况下时，获取所述付款方和所述收款方的交易信息；

所述银行区块链系统基于所述交易信息对所述收款方、所述付款方和所述交易金额进行验证；

在验证通过的情况下，更改所述付款方和所述收款方的交易状态。

[0006] 上述的系统，可选的，所述付款方基于预设媒介与所述收款方建立信息通道，包括：

所述付款方询问所述收款方的随机公钥；

所述收款方将所述随机公钥发送给所述付款方进行应答；

所述付款方基于所述随机公钥加密随机密钥发送给收款方；

所述收款方基于所述随机密钥加密回复确认应答。

[0007] 上述的系统，可选的，对所述第二数字证书和所述收款信息进行验证，包括：

对所述收款方进行验证；

获取所述收款信息中的交易金额，对所述交易金额进行验证；

基于根证书验证所述第二数字证书。

[0008] 上述的系统，可选的，所述交易回执包括：所述付款方、所述交易金额、所述收款方和所述交易标识，若所述付款方为收到所述交易回执，将所述信息通道断开，基于所述预设媒介重新建立所述付款方和所述收款方的信息通道。

[0009] 上述的系统，可选的，所述收款方中所述交易金额的交易状态为临时状态。

[0010] 一种数字货币的双离线支付方法，应用于收款方，所述方法包括：

在检测到所述收款方输入交易金额的情况下，进行广播，以令付款方与所述收款方建立信息通道；

基于所述信息通道获取所述付款方的第一数字证书，对所述第一数字证书进行验证；

验证通过后，接收所述付款方发送的数字货币和签名，对所述数字货币和所述签名进行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方。

[0011] 一种数字货币的双离线支付方法，应用于付款方，所述方法包括：

在接收到收款方广播的情况下，所述付款方基于预设媒介与所述收款方建立信息通道；

在接收到所述收款方对所述付款方验证通过指令的情况下，获取所述收款方的收款信息和所述收款方的第二数字证书，对所述第二数字证书和所述收款信息进行验证；

验证成功后，发送数字货币和签名给所述收款方，以令所述收款方对所述数字货币和所述签名进行验证，验证通过的情况下，发送交易回执；

接收所述交易回执，基于所述交易回执扣除对应交易金额。

[0012] 一种数字货币的双离线支付装置，应用于收款方，所述装置包括：

广播模块，用于在检测到所述收款方输入交易金额的情况下，进行广播，以令付款方与所述收款方建立信息通道；

验证模块，用于基于所述信息通道获取所述付款方的第一数字证书，对所述第一数字证书进行验证；

验证和发送模块，用于验证通过后，接收所述付款方发送的数字货币和签名，对所述数字货币和所述签名进行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方。

[0013] 一种数字货币的双离线支付装置，应用于付款方，所述装置包括：

建立模块，用于在接收到收款方广播的情况下，所述付款方基于预设媒介与所述收款方建立信息通道；

获取和验证模块，用于在接收到所述收款方对所述付款方验证通过指令的情况下，获取所述收款方的收款信息和所述收款方的第二数字证书，对所述第二数字证书和所述收款信息进行验证；

发送模块，用于验证成功后，发送数字货币和签名给所述收款方，以令所述收款方对所述数字货币和所述签名进行验证，验证通过的情况下，发送交易回执；

扣除模块，用于接收所述交易回执，基于所述交易回执扣除对应交易金额。

[0014] 与现有技术相比，本发明包括以下优点：

本发明公开了一种数字货币的双离线支付系统，应用于收款方和付款方，所述付款方和所述收款方组成区块链，所述系统包括：在检测到所述收款方输入交易金额的情况下，进行广播，所述付款方基于预设媒介与所述收款方建立信息通道；所述收款方基于所述信息通道获取所述付款方的第一数字证书，对所述第一数字证书进行验证；所述付款方获取所述收款方的收款信息和所述收款方的第二数字证书，对所述第二数字证书和所述收款信息进行验证；验证成功后，所述付款方发送数字货币和签名给所述收款方；所述收款方对所述数字货币和所述签名进行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方；所述付款方基于所述交易回执扣除所述交易金额，所述收款方增加所述交易金额。上述过程，实现了在没有网络条件下，基于预设媒介建立信息通道，基于信息通道实现收款方和付款方的离线支付，不受网络环境限制。

附图说明

[0015] 为了更清楚地说明本发明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。

[0016] 图1为本申请实施例公开的一种数字货币的双离线支付系统执行流程图；

图2为本申请实施例公开的一种数字货币的双离线支付方法流程图；

图3为本申请实施例公开的一种数字货币的双离线支付方法又一流程图；

图4为本申请实施例公开的一种数字货币的双离线支付装置结构框图；

图5为本申请实施例公开的一种数字货币的双离线支付装置又一结构框图。

具体实施方式

[0017] 下面将结合本发明实施例中的附图，对本发明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发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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。

[0018] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的

一般原理可以在不脱离本发明的精神或范围的情况下,在其它实施例中实现。因此,本发明将不会被限制于本文所示的这些实施例,而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

[0019] 本发明公开了一种数字货币的双离线支付系统、方法及装置,应用与数字货币的双离线支付过程中,其中,双离线支付,即不需要网络就能支付,是指收支双方都离线,也能进行支付,现有技术中,数字货币的支付采用非国密算法、不能防止双花、不能兼容基于区块链的代币并且不兼容数字身份,进一步的,在交易双方基于数字货币进行交易时,需要基于网络下可以实现付款方向收款方进行支付,在无网络条件应进行支付收到限制。基于上述的问题,本发明提供了一种数字货币的双离线支付系统,所述支付系中假设一个终端的数字货币APP一次性只能给另一个终端的数字货币 APP发送交易,所述系统支持国密SM2/SM3/SM9系列算法,在流程中通过参数可以指定使用国密算法,支持切换使用国密算法,确保了核心加密算法,数字签名算法是支持国家要求的。其中,国密算法是指国家密码局认定的国产商用密码算法,在金融领域目前主要使用公开的SM2、SM3、SM9三类算法,分别是非对称算法、哈希算法和对称算法。

[0020] 所述系统应用于收款方和付款方,所述系统在离线情况下完成支付,所述付款方和所述收款方组成区块链,所述系统的执行流程如图1所示,包括步骤:

S101、在检测到所述收款方输入交易金额的情况下,进行广播,所述付款方基于预设媒介与所述收款方建立信息通道;

本发明实施例中,在检测到所述收款方输入交易金额的情况下,所述收款方开启广播模式,广播收款信息,其中,所述收款信息包括:金额、昵称和交易ID,金额是收款方输入的,昵称不是必须的,可以是商户的名子,创建商户账号的时候商户自己输入的。所述交易ID就是一个密码学算法SM3生成的唯一的字符串。

[0021] 所述预设媒介可以为蓝牙、NFC或者红外等等,本发明实施例中以所述预设媒介为蓝牙为例进行说明,优选的,所述付款方和所述收款方均需要开启蓝牙,所述付款方扫描附近的所述收款方蓝牙信息,所述付款方主动发起连接,建立安全的信息通道(在BLE基础上应用层再封装)的步骤如下:

(1)所述付款方ask所述收款方的随机公钥(专门用于通信)。

[0022] (2)所述收款方answer所述付款方随机公钥。

[0023] (3)所述付款方使用所述付款方的随机公钥加密一个随机的密钥给所述收款方。

[0024] (4)所述收款方使用协商的密钥加密回复一个确认应答。

[0025] 进一步的,还可以协商对称加密的算法和密钥。

[0026] S102、所述收款方基于所述信息通道获取所述付款方的第一数字证书,对所述第一数字证书进行验证;

本发明实施例中,所述付款方将自己的第一数字证书基于自己的私钥加密给所述收款方,所述收款方对所述第一数字证书进行验证,所述第一数字证书里面可以验证公钥,所述第一数字证书本身可以用根证书验证,所述收款方回复加密确认。

[0027] S103、所述付款方获取所述收款方的收款信息和所述收款方的第二数字证书,对所述第二数字证书和所述收款信息进行验证;

本发明实施例中,所述付款方获取所述收款方的付款信息和所述收款方的第二数

字证书并验证收款方，验证通过的情况下，获取所述收款信息中的交易金额，对所述交易金额进行验证，验证方式可以为用户自己查看交易金额与应付金额是否相同或者在指定位置获取交易金额与应付金额进行比较，判断两者是否相同等验证方式，若所述交易金额与所述应付金额不同，说明验证不同过，反之，若所述交易金额与所述应付金额相同，则判定验证通过，验证通过的情况下，可以触发对应的验证通过指令，进一步的使用根证书验证所述第二数字证书。

[0028] S104、验证成功后，所述付款方发送数字货币和签名给所述收款方；

本发明实施例中，当所述第二数字证书和所述收款信息均验证成功后，所述付款方发送数字货币和签名给所述收款方，其中，所述数字货币的金额与所述交易金额相同，所述交易金额可以为小数或者整数，所述签名为基于自己的私钥对交易进行签名，所述签名为哈希交易串。

[0029] S105、所述收款方对所述数字货币和所述签名进行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方；

本发明实施例中，所述收款方接收所述数字货币和所述签名，并对所述数字货币和所述签名进行验证，验证过程如下，验证签名是付款方签名的，验证交易金额是正确的，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方，将交易回执发送给所述付款方，其中，所述交易回执包括：所述付款方、所述交易金额、所述收款方和所述交易标识，例如，所述交易回执为sign<付款方，交易金额，收款方，交易ID>。

[0030] S106、所述付款方基于所述交易回执扣除所述交易金额，所述收款方增加所述交易金额。

[0031] 本发明实施例中，所述付款方获取所述交易回执中的交易金额，扣除所述交易金额，所述收款方增加所述交易金额，在该种情况下，所述收款方的交易金额的状态的临时状态。

[0032] 本发明实施例中，如果所述交易回执接收不到，可以又两种颁发形式，一个是在线的，上线后，银行通知双方更新约，银行不保存余额，只是把交易信息下发，客户端更新，钱包主导货币的管理，或者银行保存余额，客户端以线上为准；一个是离线的，蓝牙重新连接后，可以再次发送回执，需要手机本地保存回执 0；

本发明公开了一种数字货币的双离线支付系统，应用于收款方和付款方，付款方和收款方组成区块链，所述系统包括：在检测到收款方输入交易金额的情况下，进行广播，付款方基于预设媒介与收款方建立信息通道；收款方基于信息通道获取付款方的第一数字证书并进行验证；付款方获取收款方的收款信息和收款方的第二数字证书并进行验证；验证成功后，付款方发送数字货币和签名给收款方令收款方进行验证，在签名和数字货币均验证通过的情况下，发送交易回执给付款方；付款方基于交易回执扣除交易金额，收款方增加交易金额。上述过程，实现了在没有网络条件下，基于预设媒介建立信息通道，基于信息通道实现收款方和付款方的离线支付，不受网络环境限制。

[0033] 本发明实施例与现有技术相比，首先，现有技术采用非国密算法，而本发明中，考虑了对国密SM2/SM3/SM9系列算法的支持，在流程中通过参数可以指定使用国密算法，支持切换使用国密算法，确保了核心加密算法，数字签名算法是支持国家要求的；现有技术中的支付过程只能保证在特定的场景下使用，比如刷公交卡，只要破译公交卡的密码，可以无限

盗刷，本发明实施例中采用数字货币，和纸币的性质一样，所有权只能从一个人转移到另一个人，一个人不能够花两次；本发明采用区块链技术，在区块链上每一笔交易都有使用者的签名，时间戳和随机数等信息，这些信息都会成用数字签名技术生成一个哈希交易串，改交易串一旦使用，就不能再次使用了，区块链上无法落账，也就花不出去；现有技术中，不能兼容基于区块链的代币，本发明实施例是基于区块链智能合约实现的，相关业务逻辑代码可以迁移到任何区块链系统上；现有技术中，不兼容数字身份，本发明实施例中，可以兼容数字身份，用户的标识使用去中心化数字身份，该身份使用密码学算法生成唯一的标识，记录在区块链上，相关的数字货币可以和身份绑定。

[0034] 本发明实施例中，所述区块链还包括：银行区块链系统，

在检测到所述区块链处于有网络情况下时，获取所述付款方和所述收款方的交易信息；

所述银行区块链系统基于所述交易信息对所述收款方、所述付款方和所述交易金额进行验证；

在验证通过的情况下，更改所述付款方和所述收款方的交易状态，优选的，所述付款方的交易金额的状态为已确认，所述收款方的交易金额的交易状态由临时状态变为可用状态。

[0035] 本发明实施例中，基于上述的一种数字货币的双离线支付系统，应用于收款方和付款方，所述付款方和所述收款方组成区块链，本发明实施例中还提供了一种数字货币的双离线支付方法，应用于收款方，所述方法的执行流程如图2所示，包括步骤：

S201、在检测到所述收款方输入交易金额的情况下，进行广播，以令付款方与所述收款方建立信息通道；

S202、基于所述信息通道获取所述付款方的第一数字证书，对所述第一数字证书进行验证，

S203、验证通过后，接收所述付款方发送的数字货币和签名，对所述数字货币和所述签名进行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方。

[0036] 本发明实施例中，所述S201-S203的支付过程与所述支付系统中针对所述收款方的处理过程相同，在此不再赘述。

[0037] 本发明公开了一种数字货币的双离线支付方法，包括：在检测到收款方输入交易金额的情况下，进行广播，付款方基于预设媒介与收款方建立信息通道；收款方基于信息通道获取付款方的第一数字证书并进行验证；付款方获取收款方的收款信息和收款方的第二数字证书并进行验证；验证成功后，付款方发送数字货币和签名给收款方令收款方进行验证，在签名和数字货币均验证通过的情况下，发送交易回执给付款方；付款方基于交易回执扣除交易金额，收款方增加交易金额。上述过程，实现了在没有网络条件下，基于预设媒介建立信息通道，基于信息通道实现收款方和付款方的离线支付，不受网络环境限制。

[0038] 本发明实施例中，基于上述的一种数字货币的双离线支付系统，应用于收款方和付款方，所述付款方和所述收款方组成区块链，本发明实施例中还提供了一种数字货币的双离线支付方法，应用于付款方，所述方法的执行流程如图3所示，包括步骤：

S301、在接收到收款方广播的情况下，所述付款方基于预设媒介与所述收款方建

立信息通道；

S302、在接收到所述收款方对所述付款方验证通过指令的情况下，获取所述收款方的收款信息和所述收款方的第二数字证书，对所述第二数字证书和所述收款信息进行验证；

S303、验证成功后，发送数字货币和签名给所述收款方，以令所述收款方对所述数字货币和所述签名进行验证，验证通过的情况下，发送交易回执；

S304、接收所述交易回执，基于所述交易回执扣除对应交易金额。

[0039] 本发明实施例中，所述S301-S304的支付过程与所述支付系统中针对所述付款方的处理过程相同，在此不再赘述。

[0040] 本发明公开了一种数字货币的双离线支付方法，包括：在检测到收款方输入交易金额的情况下，进行广播，付款方基于预设媒介与收款方建立信息通道；收款方基于信息通道获取付款方的第一数字证书并进行验证；付款方获取收款方的收款信息和收款方的第二数字证书并进行验证；验证成功后，付款方发送数字货币和签名给收款方令收款方进行验证，在签名和数字货币均验证通过的情况下，发送交易回执给付款方；付款方基于交易回执扣除交易金额，收款方增加交易金额。上述过程，实现了在没有网络条件下，基于预设媒介建立信息通道，基于信息通道实现收款方和付款方的离线支付，不受网络环境限制。

[0041] 基于上述一种数字货币的双离线支付方法，应用于收款方，本发明实施例中，还提供了一种数字货币的双离线支付装置，应用于收款方，所述支付装置的结构框图如图4所示，包括：

广播模块201、验证模块202和验证和发送模块203。

[0042] 其中，

所述广播模块201，用于在检测到所述收款方输入交易金额的情况下，进行广播，以令付款方与所述收款方建立信息通道；

所述验证模块202，用于基于所述信息通道获取所述付款方的第一数字证书，对所述第一数字证书进行验证，

所述验证和发送模块203，用于验证通过后，接收所述付款方发送的数字货币和签名，对所述数字货币和所述签名进行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方。

[0043] 本发明公开了一种数字货币的双离线支付装置，包括：在检测到收款方输入交易金额的情况下，进行广播，付款方基于预设媒介与收款方建立信息通道；收款方基于信息通道获取付款方的第一数字证书并进行验证；付款方获取收款方的收款信息和收款方的第二数字证书并进行验证；验证成功后，付款方发送数字货币和签名给收款方令收款方进行验证，在签名和数字货币均验证通过的情况下，发送交易回执给付款方；付款方基于交易回执扣除交易金额，收款方增加交易金额。上述过程，实现了在没有网络条件下，基于预设媒介建立信息通道，基于信息通道实现收款方和付款方的离线支付，不受网络环境限制。

[0044] 基于上述一种数字货币的双离线支付方法，应用于付款方，本发明实施例中，还提供了一种数字货币的双离线支付装置，应用于付款方，所述支付装置的结构框图如图5所示，包括：

建立模块301、获取和验证模块302、发送模块303和扣除模块304。

[0045] 其中，

所述建立模块301，用于在接收到收款方广播的情况下，所述付款方基于预设媒介与所述收款方建立信息通道；

所述获取和验证模块302，用于在接收到所述收款方对所述付款方验证通过指令的情况下，获取所述收款方的收款信息和所述收款方的第二数字证书，对所述第二数字证书和所述收款信息进行验证；

所述发送模块303，用于验证成功后，发送数字货币和签名给所述收款方，以令所述收款方对所述数字货币和所述签名进行验证，验证通过的情况下，发送交易回执；

所述扣除模块304，用于接收所述交易回执，基于所述交易回执扣除对应交易金额。

[0046] 本发明公开了一种数字货币的双离线支付方法，包括：在检测到收款方输入交易金额的情况下，进行广播，付款方基于预设媒介与收款方建立信息通道；收款方基于信息通道获取付款方的第一数字证书并进行验证；付款方获取收款方的收款信息和收款方的第二数字证书并进行验证；验证成功后，付款方发送数字货币和签名给收款方令收款方进行验证，在签名和数字货币均验证通过的情况下，发送交易回执给付款方；付款方基于交易回执扣除交易金额，收款方增加交易金额。上述过程，实现了在没有网络条件下，基于预设媒介建立信息通道，基于信息通道实现收款方和付款方的离线支付，不受网络环境限制。

[0047] 需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于装置类实施例而言，由于其与方法实施例基本相似，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。

[0048] 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，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、物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、物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、物品或者设备中还存在另外的相同要素。

[0049] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本发明时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0050] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例或者实施例的某些部分所述的方法。

[0051] 以上对本发明所提供的一种数字货币的双离线支付系统、方法及装置进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本

发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

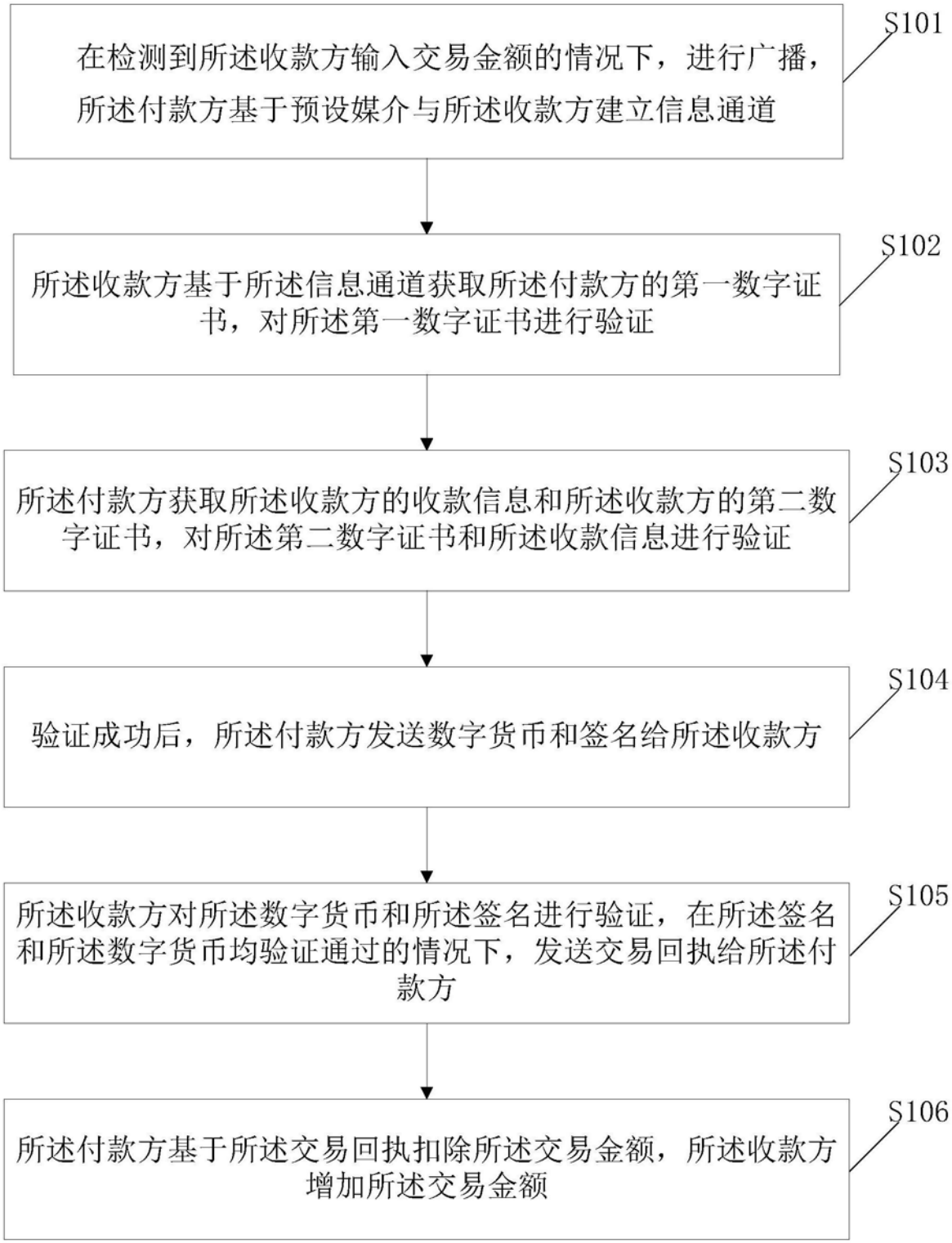

在检测到所述收款方输入交易金额的情况下，进行广播，所述付款方基于预设媒介与所述收款方建立信息通道
S101
所述收款方基于所述信息通道获取所述付款方的第一数字证书，对所述第一数字证书进行验证
S102
所述付款方获取所述收款方的收款信息和所述收款方的第二数字证书，对所述第二数字证书和所述收款信息进行验证
S103
验证成功后，所述付款方发送数字货币和签名给所述收款方
S104
所述收款方对所述数字货币和所述签名进行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方
S105
所述付款方基于所述交易回执扣除所述交易金额，所述收款方增加所述交易金额
S106

图1

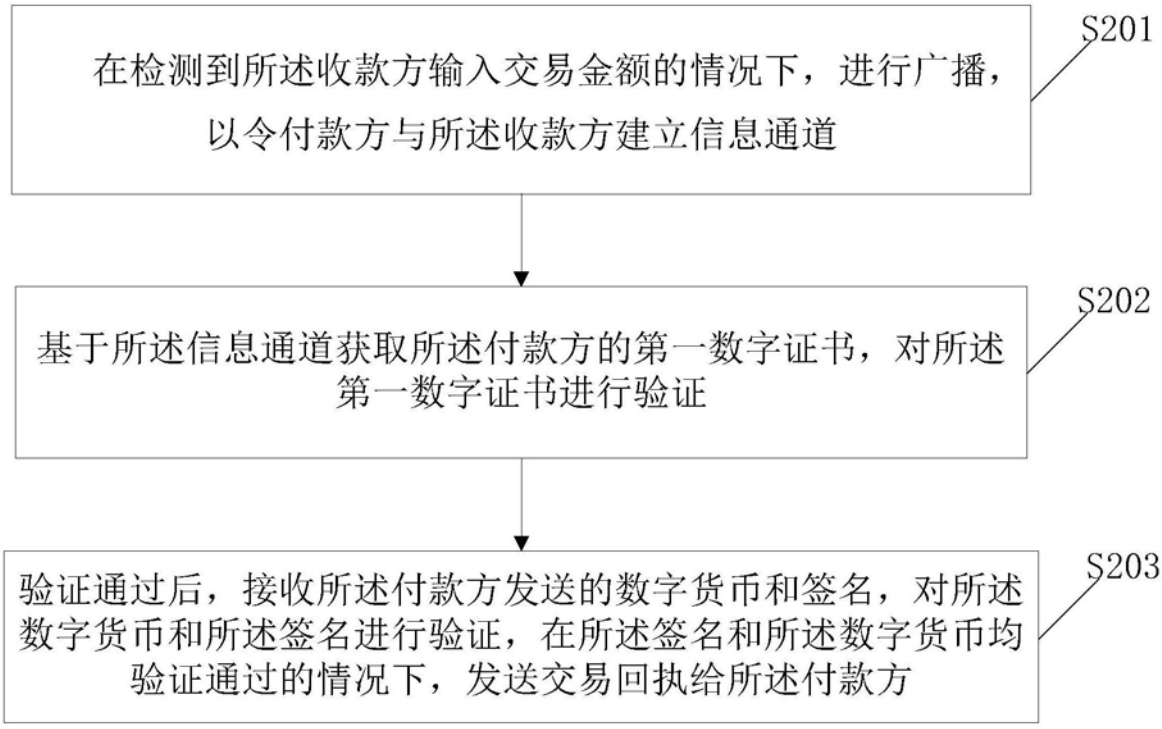

在检测到所述收款方输入交易金额的情况下，进行广播，以令付款方与所述收款方建立信息通道
S201
基于所述信息通道获取所述付款方的第一数字证书，对所述第一数字证书进行验证
S202
验证通过后，接收所述付款方发送的数字货币和签名，对所述数字货币和所述签名进行验证，在所述签名和所述数字货币均验证通过的情况下，发送交易回执给所述付款方
S203

图2

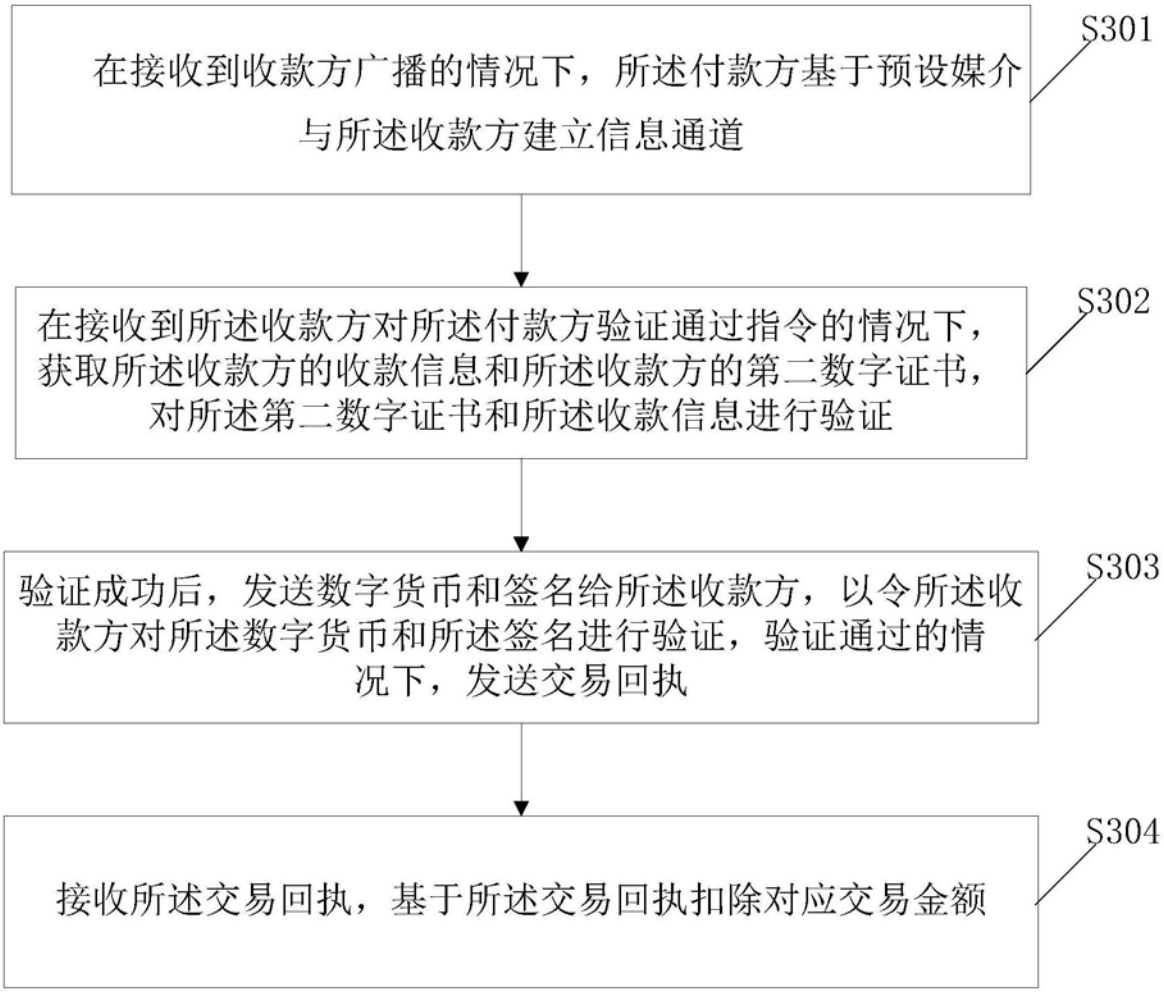

在接收到收款方广播的情况下，所述付款方基于预设媒介与所述收款方建立信息通道
S301
在接收到所述收款方对所述付款方验证通过指令的情况下，获取所述收款方的收款信息和所述收款方的第二数字证书，对所述第二数字证书和所述收款信息进行验证
S302
验证成功后，发送数字货币和签名给所述收款方，以令所述收款方对所述数字货币和所述签名进行验证，验证通过的情况下，发送交易回执
S303
接收所述交易回执，基于所述交易回执扣除对应交易金额
S304

图3

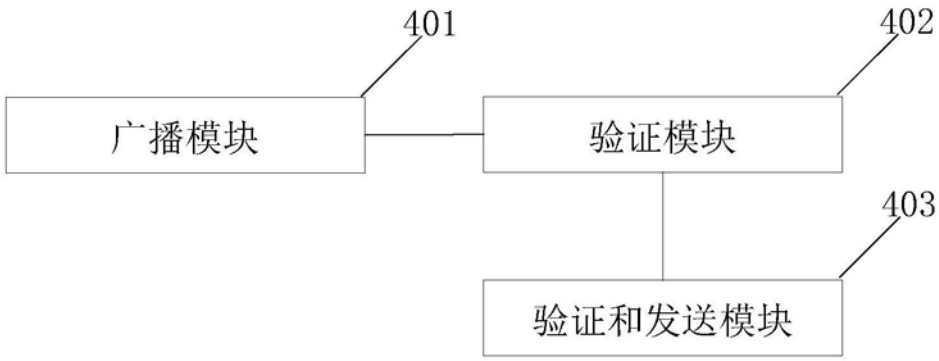

401
广播模块
402
验证模块
403
验证和发送模块

图4

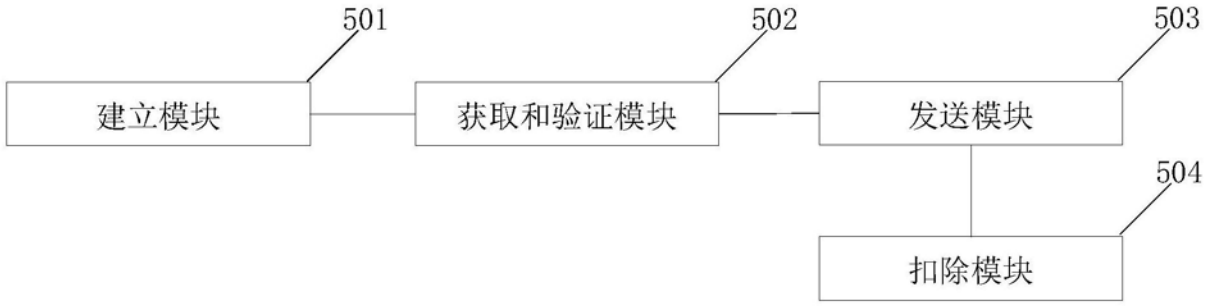


图5