



(12)发明专利申请

(10)申请公布号 CN 107230079 A

(43)申请公布日 2017.10.03

(21)申请号 201610179317.5

(22)申请日 2016.03.25

(71)申请人 中国人民银行印制科学技术研究所
地址 100070 北京市丰台区科学城中核路5号

(72)发明人 姚前 李会锋 温信祥 李连三
王栋兵 刘浩 赵欣 唐晓雪
刘文舒

(74)专利代理机构 中原信达知识产权代理有限公司
责任公司 11219

代理人 张一军 姜劲

(51)Int.Cl.

G06Q 20/36(2012.01)

G06Q 20/34(2012.01)

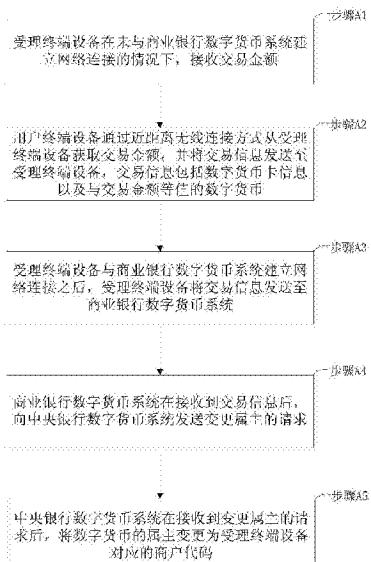
权利要求书2页 说明书23页 附图5页

(54)发明名称

使用数字货币芯片卡进行离线支付的方法及系统

(57)摘要

A
本发明提供一种使用数字货币芯片卡进行离线支付的方法及系统，该方法包括：受理终端设备在未与商业银行数字货币系统建立网络连接的情况下，接收交易金额；用户终端设备通过近距离无线连接方式从受理终端设备获取交易金额，并将交易信息发送至受理终端设备；受理终端设备与商业银行数字货币系统建立网络连接之后，受理终端设备将交易信息发送至商业银行数字货币系统；商业银行数字货币系统在接收到交易信息后，向中央银行数字货币系统发送变更属主的请求；中央银行数字货币系统在接收到变更属主的请求后，将数字货币的属主变更为受理终端设备对应的商户代码。通过本发明不仅在保证支付安全的情况下，能够有效提升了消费者在消费过程中的支付体验。



1.一种使用数字货币芯片卡进行离线支付的方法,其特征在于,包括:

受理终端设备在未与商业银行数字货币系统建立网络连接的情况下,接收交易金额;

用户终端设备通过近距离无线连接方式从所述受理终端设备获取所述交易金额,并将交易信息发送至所述受理终端设备,所述交易信息包括数字货币芯片卡信息以及与交易金额等值的数字货币;

所述受理终端设备与商业银行数字货币系统建立网络连接之后,所述受理终端设备将所述交易信息发送至所述商业银行数字货币系统;

所述商业银行数字货币系统在接收到所述交易信息后,向中央银行数字货币系统发送变更属主的请求;

所述中央银行数字货币系统在接收到所述变更属主的请求后,将所述数字货币的属主变更为所述受理终端设备对应的商户代码。

2.根据权利要求1所述的方法,其特征在于,所述近距离无线连接方式包括:NFC、红外线或蓝牙。

3.根据权利要求1所述的方法,其特征在于,所述受理终端接收所述付款信息的操作之后,还包括:

确认所述数字货币的属主与所述数字货币芯片卡相符以及确认所述交易金额与所述数字货币的币值相符。

4.根据权利要求1所述的方法,其特征在于,所述商业银行数字货币系统向中央银行数字货币系统发送变更属主的请求的操作之前,还包括:

确认所述数字货币的合法性、确认所述数字货币的属主是所述数字货币芯片卡、确认所述交易金额与所述数字货币的币值相符以及确认所述商户的账户正常使用。

5.根据权利要求1所述的方法,其特征在于,所述中央银行数字货币系统将所述数字货币的属主变更为所述受理终端设备对应的商户代码的操作之前,还包括:

确认所述数字货币的属主是所述数字货币芯片卡以及确认所述交易金额与所述数字货币的币值相符。

6.根据权利要求1所述的方法,其特征在于,所述数字货币芯片卡包括以下形态:可视蓝牙IC卡形态、IC卡形态、手机-eSE卡形态、手机-安全SD卡形态、手机-SIM卡形态。.

7.根据权利要求1所述的方法,其特征在于,所述受理终端设备是POS收款机或手机刷卡器。

8.根据权利要求1所述的方法,其特征在于,所述变更待支付的所述数字货币的属主包括:

将权属登记信息中所述数字货币的钱包地址改为所述受理终端设备对应对应的商户代码。

9.根据权利要求1所述的方法,其特征在于,将所述数字货币的属主变更为所述受理终端设备对应的商户代码的操作之后,还包括:

所述商业银行数字货币系统向所述用户终端设备和所述受理终端设备发送用于表示交易成功的提示信息。

10.一种使用数字货币芯片卡进行离线支付的系统,其特征在于,包括:用户终端设备、受理终端设备、商业银行数字货币系统以及中央银行数字货币系统,其中,

所述受理终端设备,用于在未与所述商业银行数字货币系统建立网络连接的情况下,接收交易金额,并且在与所述商业银行数字货币系统建立连接之后,所述受理终端设备将所述交易信息发送至所述商业银行数字货币系统;

所述用户终端设备,通过近距离无线连接方式从所述受理终端设备获取所述交易金额,并将交易信息发送至所述受理终端设备,所述交易信息包括数字货币芯片卡信息以及与交易金额等值的数字货币;

所述商业银行数字货币系统,用于在接收到所述交易信息后,向中央银行数字货币系统发送变更属主的请求;

所述中央银行数字货币系统,用于在接收到所述变更属主的请求后,将所述数字货币的属主变更为所述受理终端设备对应的商户代码。

11.根据权利要求10所述的系统,其特征在于,所述近距离无线连接方式包括:NFC、红外线或蓝牙。

12.根据权利要求10所述的系统,其特征在于,所述受理终端还用于:

确认所述数字货币的属主与所述数字货币芯片卡相符以及确认所述交易金额与所述数字货币的币值相符。

13.根据权利要求10所述的系统,其特征在于,所述商业银行数字货币系统还用于:

确认所述数字货币的合法性、确认所述数字货币的属主是所述付款用户、确认所述交易金额与所述数字货币的币值相符以及确认所述商户的账户正常使用。

14.根据权利要求10所述的系统,其特征在于,所述中央银行数字货币系统还用于:

确认所述数字货币的属主是所述数字货币芯片卡以及确认所述交易金额与所述数字货币的币值相符。

15.根据权利要求10所述的系统,其特征在于,所述数字货币芯片卡包括以下形态:可视蓝牙IC卡形态、IC卡形态、手机-eSE卡形态、手机-安全SD卡形态、手机-SIM卡形态。

16.根据权利要求10所述的系统,其特征在于,所述受理终端设备是POS收款机或手机刷卡器。

17.根据权利要求10所述的系统,其特征在于,所述变更待支付的所述数字货币的属主包括:

将权属登记信息中所述数字货币的钱包地址改为所述受理终端设备对应对应的商户代码。

18.根据权利要求10所述的系统,其特征在于,所述商业银行数字货币系统还用于:

向所述用户终端设备和所述受理终端设备发送用于表示交易成功的提示信息。

使用数字货币芯片卡进行离线支付的方法及系统

技术领域

[0001] 本发明涉及计算机网络以及计算机软件技术领域,具体涉及一种使用数字货币芯片卡进行离线支付的方法及系统。

背景技术

[0002] 数字货币是将现金数值转换为一系列电子加密序列数的货币,币本身的安全性依赖于密码算法来保护。在密码算法方面,数字货币系统安全性涉及到对称密码、非对称密码、报文摘要算法和基于身份的密码体制,在系统实现方面必须深入考虑密码系统的总体安全性、密码算法的选择、密码算法的实现、交互协议的设计、国际、国内标准的兼容性等,保证数字货币的交易安全。

[0003] 随着移动互联网的发展普及,移动支付产业快速变革推进,基于移动互联网、NFC、HCE、Token、生物识别等各类技术的业务模式不断创新,应用场景不断拓展丰富,线上、线下业务一体化发展加速。移动支付新技术为用户提供多元化便捷支付服务的同时,也引领着通信、金融、互联网等行业转型升级发展。移动支付广阔发展前景已成为全产业的广泛共识,移动支付被认为是连接线上线下的重要切入口。数字货币的交易系统应以移动支付为核心进行业务模式设计。

[0004] 在移动支付业务模式下,数字货币的密钥存储载体可由硬件SE模块(安全模块)、HCE以及TEE来提供。硬件SE由于其所提供的安全计算环境受到了金融交易领域的认可,在目前的借贷记卡片、电子现金中得到广泛应用,具有广泛的用户基础、良好的受理环境和使用习惯。随着移动支付技术不断发展,随着移动支付技术不断发展,SE模块形态也发生了很多变化,新的解决方案不断实践。

[0005] 在交易受理终端(POS机)和支付工具(如卡片、手机之间)的数据传输通道上,目前存在多种传输方式:RF射频通信、短信、扫码、声波、光子,多种方式的并存为支付载体间的通信提供了便利。

[0006] 在认证方式上,可分为基于口令的认证、基于口令+智能卡的认证、基于生物特征(指纹、人脸)的认证。其中口令、生物特征的认证多用于远场支付,智能卡认证多用于近场支付。

[0007] 云计算是未来后台服务器端的主流方向,数字货币的后台系统应采用基于云的解决方案。

[0008] 在电子商务活动中,因角色不同,对数字货币的要求也不同:客户要求数字货币使用方便,存储安全且具有匿名性;商家要求数字货币具有可认证性,且能兑换成真实的货币;银行则要求数字货币不能被非法使用和伪造,因此,数字货币E-RMB应具有以下特征:

[0009] 1. 安全性:能防止商务中的任意一方更改或非法使用数字货币;

[0010] 2. 不可重复花费性:数字货币只能使用一次,重复花费能被容易地检查出来;

[0011] 3. 可控匿名性:银行和商家相互勾结也不能跟踪数字货币的使用,要求系统无法将电子现金的用户的购买行为联系到一起,从而隐蔽数字货币用户的购买历史,但数字货币

币的发行方可跟踪数字货币的使用；

[0012] 4. 不可伪造性：用户不能伪造假的数字货币；

[0013] 5. 公平性：支付过程是公平的，保证要么双方交易成功，要么双方都没有损失，防止某一交易方在交易中蒙受损失；

[0014] 6. 兼容性：D-RMB系统中数字货币的发行流程与流通环节尽可能参照实物货币发行与流通。

[0015] 并且对于数字货币而言，应当能够适应于现有货币的各种使用场景，并能够与现有货币自由兑换。

[0016] 传统电子支付基于网络支付或联机刷卡支付，虽然这种电子支付方式为广大消费者提供了良好的支付方式，但是对于一些不熟悉操作或者不习惯随身携带银行卡的用户就会不太方便，因此不能很好的契合用户消费的习惯。

[0017] 鉴于上述现有技术存在的问题，亟需一种既可提供类似于纸币的当面付交易，也可提供类似于电子支付系统的网络远程支付交易的更加方便灵活的支付方式。

[0018] 此外，基于卡、终端设备等进行的移动支付需要满足更多支付场景的需要，例如在离线环境下，交易双方如何实现安全方便地交易，并且如何获得像通过纸币消费一样良好的用户体验，都是当前需要解决的技术问题。

发明内容

[0019] 有鉴于此，本发明提出一种使用数字货币芯片卡进行离线支付的方法及系统，以解决现有技术中存在的支付方式相对局限的问题。本发明的其他目的、效果以及有益效果可以从实施方式中得出。

[0020] 本发明的技术方案是提供一种使用数字货币芯片卡进行离线支付的方法，该方法包括：受理终端设备在未与商业银行数字货币系统建立网络连接的情况下，接收交易金额；用户终端设备通过近距离无线连接方式从受理终端设备获取交易金额，并将交易信息发送至受理终端设备，交易信息包括数字货币芯片卡信息以及与交易金额等值的数字货币；受理终端设备与商业银行数字货币系统建立网络连接之后，受理终端设备将交易信息发送至商业银行数字货币系统；商业银行数字货币系统在接收到交易信息后，向中央银行数字货币系统发送变更属主的请求；中央银行数字货币系统在接收到变更属主的请求后，将数字货币的属主变更为受理终端设备对应的商户代码。

[0021] 可选地，近距离无线连接方式包括：NFC、红外线或蓝牙。

[0022] 可选地，受理终端接收付款信息的操作之后，还包括：确认数字货币的属主与数字货币芯片卡相符以及确认交易金额与数字货币的币值相符。

[0023] 可选地，商业银行数字货币系统向中央银行数字货币系统发送变更属主的请求的操作之前，还包括：确认数字货币的合法性、确认数字货币的属主是数字货币芯片卡、确认交易金额与数字货币的币值相符以及确认商户的账户正常使用。

[0024] 可选地，中央银行数字货币系统将数字货币的属主变更为受理终端设备对应的商户代码的操作之前，还包括：确认数字货币的属主是数字货币芯片卡以及确认交易金额与数字货币的币值相符。

[0025] 可选地，数字货币芯片卡包括以下形态：可视蓝牙IC卡形态、IC卡形态、手机-eSE

卡形态、手机-安全SD卡形态、手机-SIM卡形态。

[0026] 可选地，受理终端设备是POS收款机或手机刷卡器。

[0027] 可选地，变更待支付的数字货币的属主包括：将权属登记信息中数字货币的钱包地址改为受理终端设备对对应的商户代码。

[0028] 可选地，将数字货币的属主变更为受理终端设备对应的商户代码的操作之后，还包括：商业银行数字货币系统向用户终端设备和受理终端设备发送用于表示交易成功的提示信息。

[0029] 本发明还提供一种使用数字货币芯片卡进行离线支付的系统，该系统包括：用户终端设备、受理终端设备、商业银行数字货币系统以及中央银行数字货币系统，其中，

[0030] 受理终端设备，用于在未与商业银行数字货币系统建立网络连接的情况下，接收交易金额，并且在与商业银行数字货币系统建立连接之后，受理终端设备将交易信息发送至商业银行数字货币系统；

[0031] 用户终端设备，通过近距离无线连接方式从受理终端设备获取交易金额，并将交易信息发送至受理终端设备，交易信息包括数字货币芯片卡信息以及与交易金额等值的数字货币；

[0032] 商业银行数字货币系统，用于在接收到交易信息后，向中央银行数字货币系统发送变更属主的请求；

[0033] 中央银行数字货币系统，用于在接收到变更属主的请求后，将数字货币的属主变更为受理终端设备对应的商户代码。

[0034] 可选地，近距离无线连接方式包括：NFC、红外线或蓝牙。

[0035] 可选地，受理终端还用于：确认数字货币的属主与数字货币芯片卡相符以及确认交易金额与数字货币的币值相符。

[0036] 可选地，商业银行数字货币系统还用于：确认数字货币的合法性、确认数字货币的属主是付款用户、确认交易金额与数字货币的币值相符以及确认商户的账户正常使用。

[0037] 可选地，中央银行数字货币系统还用于：确认数字货币的属主是数字货币芯片卡以及确认交易金额与数字货币的币值相符。

[0038] 可选地，数字货币芯片卡包括以下形态：可视蓝牙IC卡形态、IC卡形态、手机-eSE卡形态、手机-安全SD卡形态、手机-SIM卡形态。

[0039] 可选地，受理终端设备是POS收款机或手机刷卡器。

[0040] 可选地，变更待支付的数字货币的属主包括：将权属登记信息中数字货币的钱包地址改为受理终端设备对对应的商户代码。

[0041] 可选地，商业银行数字货币系统还用于：向用户终端设备和受理终端设备发送用于表示交易成功的提示信息。

[0042] 通过本发明提供的数字货币离线支付的方法及系统，由于货币本身的数字化，因此不依赖任何银行账户和单一网络，不仅在保证支付安全的情况下，能够有效提升了消费者在消费过程中的支付体验。

附图说明

[0043] 为了更清楚地说明本发明实施例中的技术方案，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。在附图中:

- [0044] 图1是与本发明实施方式有关的预制卡的工作的主要流程的示意图;
- [0045] 图2是与本发明实施方式有关的用户注册D-RMB账号的流程的示意图;
- [0046] 图3是与本发明实施方式有关的D-RMB交易过程的示意图;
- [0047] 图4是根据本发明实施方式的D-RMB数字货币系统提供在线服务时的整体框架的一种结构的示意图;
- [0048] 图5是根据本发明实施方式的商业银行数字货币系统包含的计算机系统的示意图;
- [0049] 图6是根据本发明实施方式的商业银行数字货币系统与外部系统互联的一种架构的示意图;
- [0050] 图7是根据本发明实施方式的使用数字货币芯片卡进行离线支付的方法流程图;
- [0051] 图8是根据本发明实施方式的使用数字货币芯片卡进行离线支付的系统结构图。

具体实施方式

[0052] 以下结合附图对本发明的示范性实施方式做出说明,其中包括本发明实施方式的各种细节以助于理解,应当将它们认为仅仅是示范性的。因此,本领域普通技术人员应当认识到,可以对这里描述的实施方式做出各种改变和修改,而不会背离本发明的范围和精神。同样,为了清楚和简明,以下的描述中省略了对公知功能和结构的描述。

[0053] 本发明实施方式中,描述基于密码数学的数字货币(以下简称作D-RMB)设计方案,主要运营模式是中央银行与各商业银行一起分级建设D-RMB系统。这里的中央银行是货币的发行机构,例如中国人民银行。在以下的描述中,中央银行有时简称为“央行”,类似地,商业银行有时简称为“商行”。另将数字货币表示为“D币”。

[0054] D-RMB系统是基于D币交易的资金转移系统,它由中央银行与各商业银行一起联合运营。D-RMB系统包括运行于特定数字中心的核心服务器上的D币发行、客户登录、客户账户管理、交易管理、欺诈检测、核心业务模块,也包括用户端的手机、笔记本电脑等需要与核心服务器交互的终端客户程序,同时,它还包括D币资金转移系统运行所依托的全国范围内的包括互联网、移动通信网这样一个开放形式的电子通信网络。在论述D-RMB系统之前,明确:

[0055] 1.与现有实物货币流通的兼容。D-RMB系统中数字货币的发行流程与流通环节尽可能参照实物货币发行与流通,D-RMB体系中数字货币存放历经三个环节,一是央行的数字货币发行库(即数字货币基金);二是商业银行的银行库,即商业银行的库存数字现金;三是用户端的客户应用程序,即电子钱包中。在这不同环节过程中,D-RMB的登记中心会完成相关的登记操作。

[0056] 2.D-RMB数字货币不用盲签名。在使用过程中有限度地匿名保护。

[0057] 3.D-RMB数字货币可以依托不同网络流通,以电子数字形式可能存在手机、IC卡芯片、笔记本电脑等等各种电子设备终端中,本文主要以手机和IC卡为载体存放D-RMB数字货币来进行讨论示例,但并不意味它只能以手机和IC卡为载体。

[0058] 4.D-RMB系统设计的支付模式是依靠D-RMB数字货币的转移(即:D币交易)实现。

- [0059] 5.D-RMB系统要服从我国现金管理的相关制度要求。具体要求由业务部门需求决定。
- [0060] 6.为避免与现有的记账支付体系同质化竞争,D-RMB系统可设计为限定额度支付。
- [0061] 为方便后续的描述,对以下符号约定:
- [0062] Enc:加密,这里指用户从IBC中心下载私钥后,以自己的私钥对发出信息进行签名并用对方的公钥进行加密。
- [0063] Dec:解密,这里特指用户以自己的私钥进行来文的解密,并以对方手机号作为对应公钥(或直接公钥),对用户发送的信息进行签名确认。
- [0064] D_{银行}:指银行在央行中心系统开设的准备金账户,作记账用。
- [0065] D_币:指央行按自己的加密机制生成的D-RMB数字货币,是一串字符,代表一定金额人民币。
- [0066] D_{币100}:指央行按自己的加密机制生成的D-RMB数字货币,是一串数字,代表100元人民币,依次类推,下标数字代表实际人民币数额。
- [0067] B_{账号}:用户所在开户行的银行账号。
- [0068] H(M):对M进行哈希运算得到的值,M可以是手机号、机构代码或一串字符、数字等。
- [0069] D-RMB作为数字货币,由中国人民银行作为法定货币来设立并发行进入流通,由中国人民银行作为最终贷方提供担保,参与全国标准架构内的兑、汇与消费。它是一串代码,具有与实际流通中的“面值”一样的币值意义。D-RMB数字货币模拟纸质货币在央行的发行和管理流程,在D-RMB发行库中按央行的本次数字货币发行量一次性生成数字货币。
- [0070] 在D-RMB系统设计中,D_币可以按最小单位面额产生,也可以根据用户具体提款金额来产生,也能按流通中实物货币面额产生,具体按哪种方式可通过系统参数在初始过程中设置。为贴近现实,后续以流通中固定面额为例来进行阐述。
- [0071] 发行库中的D-RMB完全模拟流通中的面值,“印制”产生数字代表的“壹圆、伍圆、拾圆、贰拾圆、伍拾圆、壹佰圆”等,一个加密文本代表一个面值的D-RMB数字货币。
- [0072] 按固定面值产生D-RMB,如按第五套生产代表D-RMB(则需生产:D_{币1}、D_{币5}、D_{币10}、D_{币20}、D_{币50}、D_{币100})则:
- [0073] 步骤1:由主密码与数字1、5、10、20、50和100分别产生六个基本加密密码。
- [0074] 步骤2:由哈希算法产生系统随机数。随机数可以理解为冠字号码。
- [0075] 步骤3:由代表不同币值的基本加密密码与随机数加密,生成加密密码。
- [0076] 步骤4:由央行私钥对加密密码进行签名,代表新币产生。假如提款人要提代表100元人民币的D_{币100},则在实际提款过程中,可由代表100元的唯一随机数字与对应基本加密密码加密生成加密密文m,再由央行私钥对m进行签名。
- [0077] 在D-RMB体系中,有央行的数字货币发行库、商业银行的数字货币银行库和用户端(如手机)的电子钱包。数字货币转移的基本内容包括:
- [0078] (1)根据数字货币发行总量,央行统一生成数字货币(即生产数字货币基金),存放在央行发行库中。
- [0079] (2)根据商业银行数字货币的需求申请,将数字货币发送到相应商业银行存放数字货币的数据库,即数字货币从发行库到银行库。
- [0080] 如某次根据货币发行总量,央行发行10亿D-RMB,这些D-RMB发行后被放在央行的

发行库中。后来根据某银行的申请从这10亿D-RMB中提走其中2亿,这些被提走的2亿D-RMB被存放在该银行的银行库中(该银行在央行的存款准备金账户记账为减少2亿,同时,2个亿的D-RMB存放在该商业银行的银行库,其记账操作等同现有实物货币的支取),在登记中心,这些数字货币对应的属主由央行改为商业银行,并记录相应操作流水等信息。

[0081] (3)用户申请提取数字货币时,数字货币从银行库到流通环节,进入用户客户端的存储介质中(如手机内),即从银行库到用户的电子钱包。在登记中心,这些数字货币对应的属主由商业银行改为用户,并记录相应操作流水等信息。

[0082] (4)在流通环节,数字货币实质是在两个用户各自电子钱包间进行转移来完成支付,此时支付分为在线交易和离线交易,具体业务流程在后文进行详细分析。在登记中心,这些数字货币对应的属主由用户1改为用户2,并记录相应操作流水等信息。

[0083] 在以上数字货币转移过程中,D-RMB系统的登记中心需验证交易数字货币的合法性,记录交易流水并更正对应数字货币新的属主,以及登记其它所需信息(具体由业务需求决定)。

[0084] 如果是以IC卡为载体,还存在预制卡的工作,预制卡的工作中,中央银行数字货币系统和商业银行数字货币系统对包含有存储介质的D-RMB芯片卡进行一系列操作,主要有:中央银行数字货币系统按预先指定的内容生成D-RMB芯片卡的个性化数据;商业银行数字货币系统将申请D-RMB芯片卡的用户的个人信息写入该D-RMB芯片卡;商业银行数字货币系统以用户IBC公钥向认证系统申请IBC私钥,用户IBC公钥是D-RMB芯片卡的标识或者所述用户的标识。以上操作中涉及的主要流程如图1所示,图1是与本发明实施方式有关的预制卡的工作的主要流程的示意图。

[0085] 卡基作为D币的安全载体,在D币流通的各个环节对于保证D币的安全性有一定加强作用(独立的物理载体IC卡也简称为“D-RMB芯片卡”)。

[0086] (1)D-RMB芯片卡的生产

[0087] D-RMB芯片卡的生产必须由经过中央银行认证的,具有生产资质的企业生产,对于其生产制造的数量以及质量由中央银行(或中央银行授权的其他部门)严格把控。企业资质认证流程包括:提交申请、材料审核、样卡检测、现场测评、授权资质等环节。

[0088] (2)D-RMB芯片卡的个性化

[0089] D-RMB芯片卡内个性化数据由中央银行生成,并授权相关部门建立个人化中心,对新生产的D-RMB芯片卡进行个性化操作。

[0090] (3)D-RMB芯片卡的发行

[0091] 系统可支持实名制发卡和匿名发卡。

[0092] 实名制发卡:D-RMB芯片卡由用户个人申请,实名制发卡,由中央银行授权商业银行代为发行,商业银行对用户进行实名审核,并登记相关资料,审核通过后,对中央银行的D-RMB芯片卡进行二次发卡,把用户的个人信息写到D-RMB芯片卡内。

[0093] 匿名发卡:用户直接向商业银行申领D-RMB芯片卡,商业银行可根据实际情况选择是否验证申请人身份信息。

[0094] 商业银行根据实际情况选择使用D-RMB芯片卡的唯一标识号或用户手机号作为用户IBC公钥,进而向IBC认证中心申请私钥。

[0095] D-RMB系统支持以计算机设备、手机、POS、ATM以及Web等方式作为载体,选择线上

或线下交易,本文示例中将主要以手机作为载体为例进行说明。

[0096] 关于手机终端,各种数字密码、图形密码等解锁设置和开机密码能有效保护手机上个人信息的安全。随着智能手机时代的到来,各类基于生物特征的指纹手机已进入普通消费群,它可以针对不同应用、不同特定信息采取不同指纹加密,这些新技术的应用可有效保证手机上数字货币、相关交易信息的存放安全。

[0097] 为确保数字货币在手机间的转移安全,D-RMB体系需引入安全认证体系。中央银行与金融机构间利用现有的CA认证中心,社会用户(包括个人和企业)可利用IBC(Identity-Based Cryptograph)认证中心进行身份认证。

[0098] 对于在IBC、PKI中产生的私钥和央行公钥,需可靠安全地存放在手机的安全专属区域SE区(Secure Element),SE区可由硬件(手机换卡)或由主机模拟卡技术HCE(Host Card Emulation)来实现。如果用户采取换卡来保护密钥,则在换卡申请过程中下载密钥到手机SE区。

[0099] 在认证体系建设过程中,可按照传统的PKI认证体系来设计,统一建立PKI体系,由CA提供强数字签名,也可以按IBC设计,以用户手机号作为公钥来管理,特别是针对微小额度的离线支付,似乎更为便捷。下文所有业务介绍将以IBC认证来进行说明。图2是与本发明实施方式有关的用户注册D-RMB账号的流程的示意图,图3是与本发明实施方式有关的D-RMB交易过程的示意图。

[0100] 在进行用户注册时,主要有以下流程:中央银行数字货币系统在接收到用户使用的终端设备发来的身份证明信息后,向该终端设备发送适用于该终端设备的应用软件;中央银行数字货币系统向运行所述应用软件的所述终端设备发送IBC公钥和IBC私钥,然后与该终端设备进行身份认证会话以及会话密钥协商;中央银行数字货币系统接收运行所述应用软件的所述终端设备发来的用户账号,然后向该终端设备发送用户密码。

[0101] 以用户1向用户2在线支付50元的数字货币D币₅₀为例,来说明交易过程中涉及D币₅₀转移时的安全协议。用户1登录自己的手机APP应用程序,完成与D-RMB系统的双方身份认证,并以SSL方式协商会话密钥后,执行交易协议。以手机号作为IBC公钥为例,在用户1手机客户端:手机客户端自动选取50元的数字货币D币₅₀,根据交易规则组织相关信息M||m,其中M可以设计为:M=交易代码||手机号1||D币₅₀||支付金额||手机号2,对信息段哈希运算得消息H(M),以手机号1对应的私钥对H(M)进行签名得m,以加密方式发送M||m到D-RMB系统。

[0102] D-RMB系统端:按协议解密报文得M||m,验证报文有效性,即以公钥即手机号1验证m与H(M),防止报文在传输过程中被篡改;验证D币₅₀是否合法,解读交易规则及相关信息,执行相应操作,主要包括业务验证后登记中心变更D币₅₀属主,由绑定的手机号1改为手机号2,并记录相应流水。发送D币₅₀给手机2,并向双方提示交易成功。

[0103] 为进一步增强匿名性,登记中心权属对应手机号可改为手机号的哈希(即借鉴比特币钱包地址,由公钥哈希组成),具体描述如下:

[0104] 客户端组织报文不变,在用户1手机客户端:自动选取50元的数字货币D币₅₀,根据交易规则组织相关信息M||m,其中M可以设计为M=交易代码||手机号1||D币₅₀||支付金额||手机号2,对信息段哈希运算得消息H(M),以手机号1对应的私钥对H(M)进行签名得m,以加密方式发送M||m到D-RMB系统。

[0105] D-RMB系统端:按协议解密报文得M||m,验证报文有效性,即以公钥即手机号1验证m

与H(M)，防止报文在传输过程中被篡改；验证D币是否合法，解读交易规则及相关信息，执行相应操作，主要包括业务验证后登记中心变更D币属主，由绑定的H(手机号1)改为H(手机号2)，并记录相应流水。发送D币给手机2，并向双方提示交易成功。

[0106] 关于系统便捷性设计，在本发明实施方式中，交易的界面和入口有多种。在场景举例过程中，仅以一个入口来举例，如注册用户在商业银行办理业务，即可由用户拿手机先直接登录D-RMB系统，也可由商业银行登录D-RMB系统。

[0107] 关于账户密码问题，可以根据业务需要来灵活设计是否需要用户输入账户密码。基于D-RMB系统是小额支付系统，建议可以考虑由用户自由选择是否设置密码。在本发明实施方式的说明中，按不留密码来描述，但在实现中，可以根据实际情况而定。

[0108] 关于客户端应用程序问题，用户可以下载相应的客户端应用程序在自己对应的终端上（此类终端软件相当于“钱包”工具），如手机用户可以下载D-RMB手机终端程序（也可称为手机APP）。终端程序可以设计包含以下功能：一是D币管理功能。（1）终端程序可以自动统计所有D币金额；（2）可以根据用户输入的金额数自动找到“钱包”内的D币组合，并在支付过程中自动选定已匹配好的D币进行交易；（3）交易完成后，自动将参与支出的D币进行删除；（4）能自动区别标识“钱包”内未经央行在线校验的数字货币和已校验已登记数字货币。二是完成业务需要的功能，如在线的注册申请、提取、支付、兑现、离线的支付请求等业务功能，以及在交易过程中自动完成公钥加密、私钥签名等等操作。

[0109] 总的说来，D-RMB体系的核心要素为一种币、两类库、三个中心：

[0110] 一种币，即“D-RMB”，也称之为D币，特指一串由央行签名的代表具体金额的加密数字串。

[0111] 两类库：分别是D-RMB的发行库和银行库。数字货币在发行库中即表现为央行的数字货币基金；数字货币在银行库中即表现为商业银行的库存数字现金。

[0112] 三个中心：一是登记中心（包括货币产生、流通、清点核对及消亡全过程记录）；另外两个是认证中心，即CA认证中心（基于PKI体系，对机构和用户证书进行集中管理，如CFCA）和IBC认证中心，即基于标识的密码技术建立的认证中心（Identity-Based Cryptograph）。在登记中心可设计两张表，一为数字货币权属登记表，记录数字货币的归属，另一张为交易流水表。

[0113] 本发明实施方式中的基于身份的密码体制IBC可以直接以用户的身份标识作为公钥，公钥的认证不再依托于证书，简化了密钥的使用与管理，具有无目录、使用方便、易于维护等优点。

[0114] 对于身份标识，个人用户可以采用手机号，也可以采用与手机匹配的E-mail地址或其他经过变换的字符串，这样方便客户本人记忆，其他人无从知道），以便达到可控匿名目的。企业用户可以采用组织机构代码，也可采用自定义的代码来作为IBC中心的身份标识，以此作为公钥，下面的举例中仅以手机号为例方便阐述。

[0115] D-RMB系统是一种分级式的体系，即由中央银行与各商业银行共建，中央银行数字货币系统是由中央银行或中央银行指定机构运行维护的用来处理关于数字货币的信息的计算机系统，其主要功能包括负责数字货币的发行与验证监测，商业银行是由商业银行或商业银行指定机构运行维护的用来处理关于数字货币的信息的计算机系统，其执行现有银行的有关货币的各种功能，即银行功能，主要包括从中央银行申请到数字货币后，负责直接

面向社会,满足提供数字货币流通服务的各项需求。

[0116] 在根据本发明实施方式的数字货币系统的基本结构中,数字货币系统主要包括中央银行数字货币系统、商业银行数字货币系统(在实际中可以是多个商业银行数字货币系统)、以及认证系统。其中,中央银行数字货币系统用于产生和发行数字货币,以及对数字货币进行权属登记;商业银行数字货币系统用于针对数字货币执行银行功能;认证系统用于对中央银行数字货币系统和数字货币的用户所使用的终端设备之间的交互提供认证,以及对中央银行数字货币系统和商业银行数字货币系统之间的交互提供认证。

[0117] 图4是根据本发明实施方式的D-RMB数字货币系统提供在线服务时的整体框架的一种结构的示意图。

[0118] 图4所示的整体框架中,D-RMB数字货币运转的核心为商业银行数字货币系统,央行D-RMB系统与商行D-RMB系统相连,负责进行交易确认。商行D-RMB系统和央行D-RMB系统都可以充分利用先进的云技术进行分散部署,同时商行D-RMB系统与其内部系统互联互通。

[0119] 从图4可以看出,商业银行数字货币系统处于核心位置与其他网络或系统相连,可应用“云计算”技术构建。D-RMB数字货币系统支持各种不同协议的网络数据,如:虚拟专用网VPN、专线、卫星网络、公共交换电话网(PSTN)、全球移动通信系统(GSM)、公共陆地移动网(PLMN),各不同网络均可实现与中心服务器直接或者间接连接。

[0120] 商行数字货币系统与央行登记中心相连,同样具备四个基本功能模块:自动跟踪账户拥有多少D-RMB数字货币的电子钱包功能模块、自动跟踪各方之间的D-RMB数字货币转移并识别可疑交易的监督功能模块、电子银行服务功能及客户关系管理CRM功能模块。

[0121] 商业银行数字货币系统中的服务器的逻辑布局采用三层架构的方式:即表示层,也就是前端应用系统200;后端应用系统202,也叫会话层、应用层,或交易逻辑层;后台数据库204为数据层。其对应的物理机器部署框图如图5所示,图5是根据本发明实施方式的商业银行数字货币系统包含的计算机系统的示意图。

[0122] 前端应用系统200是用来运行用户与货币转移服务运营商直接互动的应用程序,比如Web应用程序,此处部署的是Web服务器集群。用户和货币转移服务运营商通过用户接口和这些应用程序交互,用户接口有个人计算设备114和移动设备等。用户可以通过此入口访问电子钱包功能、监督功能、虚拟银行功能、CRM功能。Web服务器上可采用apache等开源软件。

[0123] 后端应用系统202主要用来是支持前端应用系统200的数据访问、业务逻辑处理等后台功能。此区域部署应用服务器。D-RMB数字货币可采用以Red Hat开源系统下的JBoss工具来开发应用程序。

[0124] 后台数据库204主要是数据库管理系统DBMS,包括数据仓库,存储了转移货币的销售交易、客户档案以及跟踪和调节中央银行数字货币系统进行D-RMB数字货币转移所需要的其他数据。D-RMB数字货币系统可采用以Oracle的DBMS作为数据库系统设计。

[0125] 上述商行数字货币系统能够与外部系统互联,可选的一种架构如图6所示,图6是根据本发明实施方式的商业银行数字货币系统与外部系统互联的一种架构的示意图。

[0126] 上图示范了商业银行数字货币系统与包括央行中心服务器、其他商业银行系统在内的各种外部系统适配器的物理和逻辑布局。有货币交易数据适配器、手机服务提供商SMS网关适配器、零售商系统适配器、ATM数据供应系统适配器等,通过这种互联的方式中心服

务器可以接受来自每类实体的数字货币转移请求和应答。图6充分说明了D-RMB数字货币系统对各渠道、不同协议网络的良好支持,这也是其系统具有开放性特征的表现。

[0127] 以下对IC卡为数字货币载体的业务流程加以阐述。

[0128] 在央行中心服务器设置发行库,商业银行端设置银行库。与上相同,在模拟场景的业务流程描述中,以“商业银行”作为商业银行端D-RMB系统及其内部相关系统的统称,以“中央银行”作为央行端D-RMB系统及其相关系统的统称。下面按注册(即申请领卡)、提取、支付、存款及兑现等四个重要流程,以D-RMB卡作为载体,进行面对面方式的交易来阐述。

[0129] 用户的D-RMB卡申请、提取、存款及兑现均要求在线状态下完成,而支付过程中可以分为在线支付和离线支付。用户以安全方式领取到D-RMB芯片卡后,即可向D-RMB芯片卡内存放D币。D-RMB芯片卡包含集成电路及存储介质,既可以制成单独的具有标准大小(例如目前使用的银行卡的尺寸)的卡片,也可以在集成电路的制程中集成到其他芯片或卡中。例如,D-RMB芯片卡可以是以下几种形态:可视蓝牙IC卡(以下简称可视IC卡)、普通IC卡、手机-eSE形态(手机内嵌IC卡)、手机-安全SD卡形态(内置安全SD卡)、手机-SIM卡形态以及手机-云SE形态。下面结合具体场景简要描述D币的提取,消费,存储等流程,并在相应场景中指出适用的D-RMB芯片卡形态(以下使用“全形态”来指代上面提到的所有D-RMB芯片卡形态)。

[0130] D-RMB芯片卡的申请

[0131] 流程说明:用户到商业银行柜面申请D-RMB芯片卡。

[0132] 适用D-RMB芯片卡形态:全形态

[0133] 场景说明:略。

[0134] 步骤说明:

[0135] 步骤1.用户到商业银行柜面,提交相关身份证件信息,申请D-RMB芯片卡;

[0136] 步骤2.商业银行:登记D-RMB系统页面录入申请人及卡片相关信息(如姓名、住址、电子邮件地址、手机号、身份证号、卡片号等),在商业银行D-RMB系统中为该用户创建D-RMB账号,并发送到中央银行D-RMB系统(IBC认证中心);D-RMB芯片卡可以设计为完全匿名,如果为安全匿名则无须录入申请人身份信息。本文按可控匿名设计,在后台将卡号与申请人身份信息进行绑定。

[0137] 步骤3.中央银行:在IBC中心验证其唯一性(此处以卡号为账号举例)。IBC中心:根据卡号产生用户的私钥,公钥为D-RMB芯片卡号,以公钥作为账号进行交易流转;

[0138] 步骤4.商业银行:按交易提示进行操作,下载用户私钥和央行公钥到D-RMB芯片卡保护区(写卡植密钥),完成卡的初始化,交付卡片给用户,完成重要凭证登记工作,交易结束。

[0139] 提取流程

[0140] 流程说明:用户把实物现金或其银行账户的资产转换为D币写入卡内。第一次提取流程中还包含D-RMB芯片卡申请流程,以下的描述用户已领卡之后的一些流程、场景以及步骤。

[0141] 以现金提取D币实际上也就是D币的兑换,以下加以描述。

[0142] 流程说明:用户拿实物现金提取D币到D-RMB芯片卡

[0143] 场景说明:以现金兑换D币,如用户拿250元现金到ATM或商业银行柜面(如工行网点)兑换D币,以柜面操作为例展开说明。

[0144] 适用D-RMB芯片卡形态:全形态

[0145] 步骤说明:

[0146] 步骤1. 用户向商业银行如工行某网点提交D-RMB芯片卡和现金250元要求申请兑换相应金额的D币;

[0147] 步骤2. 商业银行:清点现金,验证相关合法性(如银行库中D币是否够付等),完成自己内部系统的记账,银行库支取D币100,D币100'以及D币50;根据交易规则组织相关信息向央行D-RMB系统发送请求;

[0148] 步骤3. 中央银行:解读交易规则及相关信息,验证相关合法性(如D币100,D币100'以及D币50属主是否为工商银行等),执行相关操作,登记中心:变更D币100,D币100'以及D币50属主,将绑定的工商银行代码改为D-RMB芯片卡对应的钱包地址;记录相应交易流水;

[0149] 步骤4. 商业银行:将D币100,D币100'以及D币50写到用户D-RMB芯片卡,完成内部相应操作,交易成功打印凭条。

[0150] ATM流程基本同上。

[0151] 除了将实物现金转换为D币写入卡内,还可以从用户银行账户中转账,提取D币到D-RMB芯片卡。以下加以说明。

[0152] 流程说明:用户从B账号中转账提取D币到D-RMB芯片卡。

[0153] 适用D-RMB芯片卡形态:全形态

[0154] 场景说明:用户从工商银行账户B账号中转账提取250元D币到D-RMB芯片卡,其可通过商业银行柜面、ATM机等操作将自己的银行账户B账号转250元提取为D币写到D-RMB芯片卡内。不同渠道读写卡设备不同,大体流程相同,这里不一一进行阐述,仅以银行柜面操作为例进行说明。

[0155] 步骤说明:

[0156] 步骤1. 用户:向商业银行柜面柜员提出250元提取D币申请,提交银行卡以及D-RMB芯片卡,填写有关单据,输入B账号账户密码;

[0157] 步骤2. 商业银行:验证相关合法性,如核验账户密码、用户资金账户即B账号余额是否够付、银行库中D币是否够付等;检查通过后B账号扣款250元,银行库支取D币100,D币100'以及D币50;根据交易规则组织相关信息向央行D-RMB系统发送请求;

[0158] 步骤3. 中央银行:解读交易规则及相关信息,验证相关合法性(如D币100,D币100'以及D币50属主是否为工商银行等),执行相关操作,登记中心:变更D币100,D币100'以及D币50属主,将绑定的工商银行代码改为D-RMB芯片卡的钱包地址;记录相应交易流水;

[0159] 步骤4. 商业银行:将D币100,D币100'以及D币50写到用户D-RMB芯片卡,完成内部相应操作,交易成功打印凭条。

[0160] 本流程不仅是一个用户提款流程,同时也是一个D-RMB数字货币从银行库到用户端的流程,即法定数字货币的进入流通领域流程。

[0161] 以下对基于D-RMB芯片卡的支付流程加以说明。用户持D-RMB芯片卡支付交易,可以是持卡在联网的商家POS机上消费,可以是持卡对在线的手机进行支付,也支持卡在网上支付消费(线上支付)。另外,离线场景下还支持持卡对脱机POS支付、对无信号的手机支付,支持卡对卡的支付。这些支付过程还可细分为全款支付和找零支付,下面将一一说明。

[0162] 流程说明:D-RMB芯片卡在商家POS机上联机支付。

[0163] 场景说明:联机支付也叫在线支付,涉及全款支付和找零支付两种场景。例如付款用户D-RMB芯片卡1有数字货币 $D_{币100}, D_{币100}'$, $D_{币50}$,分别代表其拥有100元人民币两张和一张50元人民币,共计250元人民币,现需支付给收款商家用户2(POS机2)200元人民币,还需支付给另一收款商家用户3(POS机3)30元人民币。假设POS机商家用户为工商银行客户。用户D-RMB芯片卡1支付给POS机2是全款支付,用户1支付给POS机3是找零支付。找零支付可以与实物货币一样,POS机3如有 $D_{币20}$,可先由用户D-RMB芯片卡1付款50元给商家POS机3,再由商家POS机3付款20元给用户D-RMB芯片卡1,即通过两次全款支付实现(如果数字货币按照最小单位发行,则不存在找零问题),或者通过用户D-RMB芯片卡1先向D-RMB系统申请零钱兑换,再将兑换后的零钱选择组合全款支付给商家POS机3。

[0164] 适用D-RMB芯片卡形态:全形态,包括手机在内。

[0165] 步骤说明(全款支付):

[0166] 步骤1.POS机2:在POS输入消费金额200元;

[0167] 步骤2.D-RMB芯片卡1:通过NFC等无线接口与POS机通信,自动选取金额为200元的数字货币 $D_{币100}, D_{币100}'$,发送给POS机;

[0168] 步骤3.POS机2:收 $D_{币100}, D_{币100}'$,进行相关合法性检查,如初步验卡验D-RMB并判断金额是否足够等,根据交易规则组织相关信息发送到商业银行D-RMB系统;

[0169] 步骤4.商业银行:解读交易规则及相关信息,验证相关合法性(如 $D_{币100}, D_{币100}'$ 合法性,交易金额是否与数字货币币值相符等),执行相应操作,并根据交易规则重新组织报文向央行D-RMB系统发送请求;

[0170] 步骤4.中央银行:解读交易规则及相关信息,验证相关合法性(如 $D_{币100}, D_{币100}'$ 属主是否为D-RMB芯片卡1等),执行相关操作,登记中心:变更 $D_{币100}, D_{币100}'$ 属主,将绑定的D-RMB芯片卡1钱包地址改为POS机2对应的商家代码;记录相应交易流水;

[0171] 步骤5.商业银行:发送 $D_{币100}, D_{币100}'$ 到POS机2,发送交易成功的提示信息。

[0172] 步骤6.POS机2:打凭条,交易完成。

[0173] 以上完全模拟商家接收实物现金过程,在此过程中POS机2上存放 $D_{币}$ 。此过程还可设计成商家自动将 $D_{币}$ 转存到结算账户。具体如下:

[0174] 步骤1.POS机2:在POS输入消费金额200元;

[0175] 步骤2.D-RMB芯片卡1:通过NFC等无线接口与POS机通信,自动选取金额为200元的数字货币 $D_{币100}, D_{币100}'$,发送给POS机;

[0176] 步骤3.POS机2:进行相关合法性检查,如初步验卡验D-RMB并判断金额是否足够等,根据交易规则组织相关信息发送到商业银行D-RMB系统;

[0177] 步骤4.商业银行:解读交易规则及相关信息,验证相关合法性(如 $D_{币100}, D_{币100}'$ 合法性,交易金额是否与数字货币币值相符等),执行相应操作,银行库收 $D_{币100}, D_{币100}'$,并根据交易规则重新组织报文向央行D-RMB系统发送请求;

[0178] 步骤5.中央银行:解读交易规则及相关信息,验证相关合法性(如 $D_{币100}, D_{币100}'$ 属主是否为D-RMB芯片卡1等),执行相关操作,登记中心:变更 $D_{币100}, D_{币100}'$ 属主,将绑定的D-RMB芯片卡1钱包地址改为商家账号对应的商业银行代码;记录相应交易流水;

[0179] 步骤6.商业银行:将商家用户银行账号内金额增加200元,反馈相关信息;

[0180] 步骤7.POS机2:打凭条,交易完成。

- [0181] 步骤说明(零钱兑换):
- [0182] 步骤1.POS机3:插D-RMB芯片卡,选择功能“整换零”,输入:兑换金额(如50元),面值要求(如20元两枚,10元一枚);点击“发送”;
- [0183] 步骤2.D-RMB芯片卡及POS机3:自动选取50元的数字货币如D_{币50},根据交易规则组织相关信息,并发送到商业银行D-RMB系统;
- [0184] 步骤3.商业银行:解读交易规则及相关信息,验证相关合法性(如D_{币50}合法性,交易金额是否与数字货币币值相符等),执行相应操作,银行库:收D_{币50},支取D_{币20}、D_{币20'}、D_{币10};并根据交易规则重新组织报文向央行D-RMB系统发送请求;
- [0185] 步骤4.中央银行:解读交易规则及相关信息,验证相关合法性(如D_{币20}、D_{币20'}、D_{币10}以及D_{币50}属主是否合法等),执行相关操作,登记中心:变更D_{币20}、D_{币20'}、D_{币10}以及D_{币50}属主,将D_{币50}绑定的D-RMB芯片卡1钱包地址改为工商银行代码,D_{币20}、D_{币20'}、D_{币10}绑定的工商银行代码变更为D-RMB芯片卡1钱包地址;记录相应交易流水;
- [0186] 步骤5.商业银行:发送D_{币20}、D_{币20'}、D_{币10}到POS机3写D-RMB芯片卡1,发送交易成功信息。
- [0187] 其它交易流程同全款支付。即:
- [0188] 步骤6.POS机3:在POS输入消费金额30元;
- [0189] 步骤7.D-RMB芯片卡1:通过NFC等无线接口与POS机通信,自动选取金额为30元的数字货币D_{币20}、D_{币10};发送给POS机;
- [0190] 步骤8.POS机3:收D_{币20}、D_{币10},进行相关合法性检查,如初步验卡验D-RMB并判断金额是否足够等,根据交易规则组织相关信息发送到商业银行D-RMB系统;
- [0191] 步骤9.商业银行:解读交易规则及相关信息,验证相关合法性(如D_{币20}、D_{币10}合法性,交易金额是否与数字货币币值相符等),执行相应操作,并根据交易规则重新组织报文向央行D-RMB系统发送请求;
- [0192] 步骤10.中央银行:解读交易规则及相关信息,验证相关合法性(如D_{币20}、D_{币10}属主是否为D-RMB芯片卡1等),执行相关操作,登记中心:变更D_{币20}、D_{币10'}属主,将绑定的D-RMB芯片卡1钱包地址改为POS机3对应的商家代码;记录相应交易流水;
- [0193] 步骤11.商业银行:发送D_{币20}、D_{币10}到POS机3,发送交易成功的提示信息。
- [0194] 步骤12.POS机3:打凭条,交易完成。
- [0195] 在具体应用程序开发过程中以上可设计为程序联动处理。
- [0196] 流程说明:可视D-RMB芯片卡在手机上在线支付。
- [0197] 场景说明:付款用户可视D-RMB芯片卡1有数字货币D_{币100},D_{币100'},D_{币50},分别代表其拥有100元人民币两张和一张50元人民币,共计250元人民币,现需支付给收款用户2(手机2)200元人民币。
- [0198] 适用D-RMB芯片卡形态:可视D-RMB芯片卡
- [0199] 步骤说明:
- [0200] 步骤1.D-RMB芯片卡1:输入金额200元,通过蓝牙、NFC等无线技术与手机通信,自动选取金额为200元的数字货币D_{币100}、D_{币100'},发送给手机;
- [0201] 步骤2.手机2:收D_{币100}、D_{币100'},进行相关合法性检查,如初步验卡验D-RMB并判断金额是否足够等,根据交易规则组织相关信息发送到商业银行D-RMB系统;

[0202] 步骤3.商业银行:解读交易规则及相关信息,验证相关合法性(如D_{币100}’、D_{币100}合法性,交易金额是否与数字货币币值相符、手机2是否为注册用户等),执行相应操作,并根据交易规则重新组织报文向央行D-RMB系统发送请求;

[0203] 步骤4.中央银行:解读交易规则及相关信息,验证相关合法性(如D_{币100}’、D_{币100}属主是否为D-RMB芯片卡1,交易金额是否与数字货币币值相符等),执行相关操作,登记中心:变更D_{币100}’、D_{币100}属主,将绑定的D-RMB芯片卡1钱包地址改为用户2钱包地址;记录相应交易流水;

[0204] 步骤5.商业银行:向手机2反馈交易成功信息,若D-RMB芯片卡申请过程中预留并通过手机提醒业务,则同时向D-RMB芯片卡对应手机发送交易相关信息;

[0205] 步骤6.手机2:向D-RMB芯片卡反馈交易OK,交易成功。

[0206] 流程说明:开通过手机提醒的D-RMB芯片卡在手机上在线支付。

[0207] 场景说明:付款用户D-RMB芯片卡1在申请过程中已预留手机号并开通短信通知功能,D-RMB芯片卡1有数字货币D_{币100},D_{币100}’,D_{币50},分别代表其拥有100元人民币两张和一张50元人民币,共计250元人民币,现需支付给收款用户2(手机2)200元人民币。

[0208] 适用D-RMB芯片卡形态:手机、开通过手机短信提醒服务的D-RMB芯片卡。

[0209] 步骤说明:

[0210] 步骤1.手机2:选择功能菜单“对方卡支付”,输入支付金额200元;

[0211] 步骤2.D-RMB芯片卡1:通过蓝牙、NFC等无线技术与手机通信,自动选取金额为200元的数字货币D_{币100}’、D_{币100},发送给手机;

[0212] 步骤3.手机2:收D_{币100}’、D_{币100},进行相关合法性检查,如初步验卡验D-RMB并判断金额是否足够等,根据交易规则组织相关信息发送到商业银行D-RMB系统;

[0213] 步骤4.商业银行:解读交易规则及相关信息,验证相关合法性(如D-RMB芯片卡1是否有对应手机短信提醒功能,交易金额是否与数字货币币值相符等,为加强风控管理,还可加入与D-RMB芯片卡1注册手机的交易确认),执行相应操作,并根据交易规则重新组织报文向央行D-RMB系统发送请求;

[0214] 步骤5.中央银行:解读交易规则及相关信息,验证相关合法性(如D_{币100}’、D_{币100}属主是否为D-RMB芯片卡1,交易金额是否与数字货币币值相符等),执行相关操作,登记中心:变更D_{币100}’、D_{币100}属主,将绑定的D-RMB芯片卡1钱包地址改为用户2钱包地址;记录相应交易流水;

[0215] 步骤6.商业银行:向手机2反馈交易成功信息,向D-RMB芯片卡对应手机发送交易相关信息。

[0216] 此处流程也可设计为D-RMB芯片卡对应手机参与交易的确认,具体细节可由业务部门确定。

[0217] 流程说明:D-RMB芯片卡在网上线上支付。

[0218] 场景说明:付款用户D-RMB芯片卡1有数字货币D_{币100},D_{币100}’,以及D_{币50},分别代表其拥有100元人民币两张和一张50元人民币,共计250元人民币,现在通过个人终端读卡器或手机联线上网,在网上进行在线购物,需支付给收款商家用户250元人民币。

[0219] 使用D-RMB芯片卡形态:全形态

[0220] 步骤说明:

- [0221] 步骤1.付款用户:在某商家购物网站或APP选定商品,选择D币支付;
- [0222] 步骤2.商家用户:调用D-RMB系统支付插件,获取D-RMB芯片卡相关信息以及其内的D币100、D币100'、D币50,进行相关合法性检查,如初步验卡验D-RMB并判断金额是否足够等,根据交易规则组织包括商家银行账户信息在内的相关信息发送到商业银行D-RMB系统;
- [0223] 步骤3.商业银行:解读交易规则及相关信息,验证相关合法性(如D币100、D币100'、D币50合法性,交易金额是否与数字货币币值相符、商家银行账号是否可用等),执行相应操作,银行库:收D币100、D币100'、D币50,并根据交易规则重新组织报文向央行D-RMB系统发送请求;
- [0224] 步骤4.中央银行:解读交易规则及相关信息,验证相关合法性(如D币100、D币100'、D币50属主是否为D-RMB芯片卡1,交易金额是否与数字货币币值相符等),执行相关操作,登记中心:变更D币100、D币100'、以及D币50属主,将绑定的D-RMB芯片卡1钱包地址改为商户账号对应的开户银行代码;记录相应交易流水;
- [0225] 步骤5.商业银行:在商家账户内增加相应金额(250元),通知商户收款成功;
- [0226] 步骤6.商家用户:线上支付交易成功、线下组织发货,相关信息反馈付款用户;
- [0227] 如果涉及找零操作,可参照前文描述的POS在线支付流程。
- [0228] 以上重点描述了D-RMB芯片卡的在线支付几个典型应用场景中的流程和具体步骤,下面将针对D-RMB芯片卡的离线支付,包括在离线POS机、无网络信号的手机以及卡与卡之间离线支付等典型应用场景进行描述。
- [0229] 在D-RMB系统中定义的离线支付指的是近场支付,此过程中,接收方需事后联机确认收款。与前文流程一样,离线支付过程中,收款用户对收到的D币当时能验证数字货币的真伪,但仍需对D币是否进行过重复支付开展后台验证。其设计思路是:需重复支付验证的D币在客户端电子钱包程序(如POS机)中标识为“待重复支付验证”,POS机一旦联到网络,就自动向D-RMB系统进行重复支付验证申请。D-RMB系统收到验证申请执行相应操作,在登记中心补录交易流水,更新D币属主。如收款人不是D-RMB系统的注册用户,系统还会记录收款人预留的取款密码,以下将作具体说明。
- [0230] 流程说明:D-RMB芯片卡在商家POS机上离线支付。
- [0231] 场景说明:付款用户D-RMB芯片卡1有数字货币D币100,D币100',以及D币50,分别代表其拥有100元人民币两张和一张50元人民币,共计250元人民币,现需支付给收款商家用户2(POS机2)200元人民币,商家用户POS机脱机状态。
- [0232] 适用D-RMB芯片卡形态:全形态,包括手机在内。
- [0233] 步骤说明:
- [0234] 步骤1.POS机2:在POS选择离线支付,输入消费金额200元;
- [0235] 步骤2.D-RMB芯片卡1:通过NFC等无线接口与POS机通信,自动选取金额为200元的数字货币D币100',D币100,发送给POS机;
- [0236] 步骤3.POS机2:收D币100',D币100,进行相关合法性检查,如验卡验D-RMB并判断金额是否足够等,校验通过后当面交易结束,打印凭条。POS机一旦联到网络,就自动向商业银行D-RMB系统进行重复支付验证申请,根据交易规则组织相关信息发送到商业银行D-RMB系统;
- [0237] 步骤4.商业银行:解读交易规则及相关信息,验证相关合法性(如D币100',D币100合法性,交易金额是否与数字货币币值相符等),执行相应操作,并根据交易规则重新组织报文

向央行D-RMB系统发送请求；

[0238] 步骤5.中央银行:解读交易规则及相关信息,验证相关合法性(如D_{币100},D_{币100'}属主是否为D-RMB芯片卡1等),执行相关操作,登记中心:变更D_{币100'}、D_{币100}属主,将绑定的D-RMB芯片卡1钱包地址改为POS机2对应的商家代码;记录相应交易流水;

[0239] 步骤6.商业银行:向POS机2反馈验证成功信息。

[0240] 以上完全模拟商家接收实物现金过程,在此过程中POS机2上存放D_币。此过程还可设计成商家自动将D_币转存到结算账户。具体如下:

[0241] 步骤1.POS机2:一旦联网,就根据交易规则将交易信息、收到所有D_币信息和商家用户银行账号等相关信息自动发送到商业银行;

[0242] 步骤2.商业银行:进行相关合法性验证,银行库:收D_{币100},D_{币100'},根据交易规则组织相关信息发送到中央银行D-RMB系统;

[0243] 步骤3.中央银行:解读交易规则及相关信息,验证相关合法性(如D_币属主是否为D-RMB芯片卡1,交易金额是否与数字货币币值相符等),执行相应操作。登记中心:变更D_{币100'}、D_{币100}属主,将绑定的D-RMB芯片卡1钱包地址改为商家账号对应的商业银行代码;记录相应交易流水;

[0244] 步骤4.商业银行:将商家用户银行账号内金额增加相应金额,反馈相关信息;

[0245] 步骤5.POS机2:打入账凭条,交易完成。

[0246] 流程说明:D-RMB芯片卡在手机上离线支付。

[0247] 适用D-RMB芯片卡形态:可视D-RMB芯片卡。

[0248] 场景说明:根据收款用户是否为注册用户,分两种场景讨论。付款可视D-RMB芯片卡1有数字货币D_{币100},D_{币100'},D_{币50},分别代表其拥有100元人民币两张和一张50元人民币,共计250元人民币,现需离线支付给收款用户2(手机号2)200元人民币,还需离线支付给另一收款用户3(手机号3)50元人民币。其中,用户2是D-RMB系统的注册用户,而用户3没有注册,仅是在手机3上下载有D-RMB客户端。

[0249] 向用户2离线支付步骤说明(付款人和收款人都是注册用户):

[0250] 步骤1.D-RMB芯片卡:输入付款金额(如200元),通过蓝牙、NFC等无线技术与手机通信,自动选取金额为200元的数字货币D_{币100'}以及D_{币100},发送给手机;

[0251] 步骤2.用户2手机客户端:解读交易规则及相关信息,验证相关合法性(如D_{币100'}、D_{币100}合法性,交易金额是否相符等),通过后当面交易结束。待联机状态下将带有付款用户D-RMB芯片卡1签名的含D_币支付交易信息上报商业银行D-RMB系统(终端设计可自动联网验证);

[0252] 步骤3.商业银行:解读交易规则及相关信息,验证相关合法性(如D_{币100'}、D_{币100}合法性,交易金额是否与数字货币币值相符等),执行相应操作,并根据交易规则重新组织报文向央行D-RMB系统发送请求;

[0253] 步骤4.中央银行:解读交易规则及相关信息,验证相关合法性(如D_{币100},D_{币100'}属主是否为D-RMB芯片卡1等),执行相关操作,登记中心:变更D_{币100'}、D_{币100}属主,将绑定的D-RMB芯片卡1钱包地址改为用户2钱包地址;记录相应交易流水;

[0254] 步骤5.商业银行:发送信息提示验证成功。

[0255] 向用户3离线支付步骤说明(收款人是非注册用户):

[0256] 步骤1. 用户3手机客户端:登录手机客户端APP,选择功能“非注册用户离线收款”,输入:收款金额(如50元)、收款人留的pin码(由用户3输入,为证明取款人身份用),点击“开始读卡”;

[0257] 步骤2.D-RMB芯片卡:输入付款金额(如50元),通过蓝牙、NFC等无线技术与手机通信,自动选取金额为50元的数字货币D_{币50},开始与手机通信;

[0258] 步骤3.用户3手机客户端:解读交易规则及相关信息,验证相关合法性(如D_{币50}合法性,交易金额是否相符等),通过后当面交易结束。在联机状态下自动将带有付款D-RMB芯片卡签名,含D_币支付交易信息以及个人预留密码的有关信息上报商业银行D-RMB系统;

[0259] 步骤4.商业银行:解读交易规则及相关信息,验证相关合法性(如D_{币50}合法性,交易金额是否与数字货币币值相符等),执行相应操作,并根据交易规则重新组织报文向央行D-RMB系统发送请求;

[0260] 步骤5.中央银行:解读交易规则及相关信息,验证相关合法性(如D_{币50}属主是否为D-RMB芯片卡1等),执行相关操作,登记中心:对D_币属主进行更新,并留下收款人的密码;记录相应交易流水;

[0261] 步骤6.商业银行:发送信息提示验证成功并注意保管好密码。收款人在兑现时,需出示自己手机号及正确的预留密码。

[0262] 流程说明:D-RMB芯片卡对D-RMB芯片卡的离线支付。

[0263] 适用D-RMB芯片卡形态:可视D-RMB芯片卡。

[0264] 场景说明:付款可视D-RMB芯片卡1有数字货币D_{币100},D_{币100'},以及D_{币50},分别代表其拥有100元人民币两张和一张50元人民币,共计250元人民币,现需离线支付给可视收款D-RMB芯片卡2人民币200元。

[0265] 步骤1.D-RMB芯片卡1:输入付款金额(如200元),通过蓝牙、NFC等无线技术与手机通信,自动选取金额为200元的数字货币D_{币100'}以及D_{币100},发送给D-RMB芯片卡2;

[0266] 步骤2.D-RMB芯片卡2:解读交易规则及相关信息,验证相关合法性(如D_{币100'}、D_{币100}合法性,交易金额是否相符等),通过后显示收款金额200,当面交易结束。待联机状态下(如通过个人终端读卡器联网)将带有付款用户D-RMB芯片卡1签名的含D_币支付交易信息上报商业银行D-RMB系统;

[0267] 步骤3.商业银行:解读交易规则及相关信息,验证相关合法性(如D_{币100'}、D_{币100}合法性,交易金额是否与数字货币币值相符等),执行相应操作,并根据交易规则重新组织报文向央行D-RMB系统发送请求;

[0268] 步骤4.中央银行:解读交易规则及相关信息,验证相关合法性(如D_{币100},D_{币100'}属主是否为D-RMB芯片卡1等),执行相关操作,登记中心:补记相应流水,更新D_{币100'}、D_{币100}属主,将绑定的D-RMB芯片卡1钱包地址改为D-RMB芯片卡2钱包地址;

[0269] 步骤5.商业银行:发送信息提示验证成功并写D-RMB芯片卡2上D_币状态为验证通过可正常使用。

[0270] 关于离线支付过程中的找零问题,因为是完全模拟面值发行,则如同现金交易,在有零钱条件下可按双向全款支付设计来实现找零。如果数字货币按照最小单位发行,则不存在找零问题。

[0271] 以下再对存款流程加以说明。

[0272] 流程说明:用户将D-RMB芯片卡内D币存入银行账号。

[0273] 适用D-RMB芯片卡形态:全形态

[0274] 场景说明:用户的D-RMB芯片卡1有数字货币D币100,D币100',D币50,分别代表其拥有100元人民币两张和一张50元人民币,共计250元人民币,其可通过商业银行柜面、ATM机、网上银行或手机银行操作将D币存储到自己的银行账户B账号中,不同渠道读卡设备不同,大体流程相同,这里不一一进行阐述,仅以ATM机为例进行步骤说明。

[0275] 步骤说明:

[0276] 步骤1.用户向ATM机中插入银行卡以及D-RMB芯片卡(ATM也支持挥卡操作,所以也能够支持手机-XX形态的D-RMB芯片卡),选择D-RMB存款业务;

[0277] 步骤2.ATM机:提示用户输入存款金额;

[0278] 步骤3.用户:输入存款金额250元,并点击确定;

[0279] 步骤4.ATM机:ATM从D-RMB芯片卡内取出D币100、D币100'、D币50,并验证真伪以及属主,验证通过后,将银行卡号及D币100、D币100'、以及D币50根据交易规则组织相关信息发送到银行卡开户商业银行D-RMB系统;

[0280] 步骤5.商业银行:解读交易规则及相关信息,验证相关合法性(如D币100、D币100'、D币50合法性,银行卡合法性,交易金额是否与数字货币币值相符等),执行相应操作,银行库:收D币100、D币100'、D币50,并根据交易规则重新组织报文向央行D-RMB系统发送请求;

[0281] 步骤6.中央银行:解读交易规则及相关信息,验证相关合法性(如D币100、D币100'、D币50属主是否为D-RMB芯片卡1等),执行相关操作,登记中心:更新D币100、D币100'、D币50属主,将绑定的D-RMB芯片卡1钱包地址改为对应商业银行代码;记录相关流水;

[0282] 步骤7.商业银行:在用户的B账户中增加250元;反馈相关信息;

[0283] 步骤8.ATM机:提示存款完成,请用户取回银行卡以及D-RMB芯片卡。

[0284] 以下再对兑现流程加以说明。

[0285] 流程说明:用户将D-RMB芯片卡内D币兑换为实物现金。

[0286] 适用D-RMB芯片卡形态:全形态

[0287] 场景说明:用户的D-RMB芯片卡1有数字货币D币100,D币100',D币50,

[0288] 分别代表其拥有100元人民币两张和一张50元人民币,共计250元人民币,其可通过商业银行柜面、ATM机申请将D币兑换为实物现金,现以ATM机兑换100元纸币为例进行步骤说明。

[0289] 步骤说明:

[0290] 步骤1.用户将D-RMB芯片卡插入ATM,(ATM也支持挥卡操作,所以也能够支持手机-XX形态的D-RMB芯片卡)选择兑换现金业务,输入兑换金额为100元;

[0291] 步骤2.ATM及D-RMB芯片卡:自动选取金额为100元数字货币D币100,根据交易规则组织相关信息发送到商业银行D-RMB系统;

[0292] 步骤3.商业银行:解读交易规则及相关信息,验证相关合法性(如D币100合法性,交易金额是否与数字货币币值相符等),执行相应操作,银行库:收D币100,并根据交易规则重新组织报文向央行D-RMB系统发送请求;

[0293] 步骤4.中央银行:解读交易规则及相关信息,验证相关合法性(如D币100属主是否为D-RMB芯片卡1等),执行相关操作,登记中心:更新D币100属主,将绑定的D-RMB芯片卡1钱包地

址改为对应商业银行代码;记录相关流水;

[0294] 步骤5. 商业银行:反馈相关信息;

[0295] 步骤6. ATM:点钞吐给用户100元纸币;退回完成交易。

[0296] 以下再对D-RMB芯片卡作为数字货币载体时的重复交易检测加以说明。在本发明实施方式中,即在线交易情况下,D-RMB系统通过D币与用户卡号11绑定方式来防重复交易。D-RMB系统中登记中心有一权属登记表,记录表样式可设计如表1:

[0297] 表1:

[0298]

数字货币名	属主	备注
Pbc100adfk109987766670	ICC00000001	D币100
.....
Pbc50cadfk109987766670	ICC00000002	D币50

[0299] 用户D-RMB芯片卡1(D-RMB芯片卡唯一标识号ICC00000001)在向用户D-RMB芯片卡2(D-RMB芯片卡唯一标识号ICC00000002)支付D币100过程中,D-RMB系统登记中心权属登记表:更改D币100对应属主,将属主字段中原手机号ICC00000001对应的钱包地址更改为手机号ICC00000002对应的钱包地址,如果用户D-RMB芯片卡1还想用D币100向其它用户D-RMB芯片卡支付,此时其属主已不是用户D-RMB芯片卡1,无法完成支付,以此来防止重复支付。

[0300] 离线交易情况下,通过滞后重复支付检查来发现并追责,目前几乎所有的电子现金系统进行的重复支付检查都是滞后的,即重复支付检查都是在支付过程完成后进行的。

[0301] 同时可设定的交易为小额支付(小于1000元),对于个人用户是一个可以接受的范围,并且采用事后追责机制,对不良记录将录入征信系统以作惩戒。

[0302] 以下再对本发明实施方式中的使用数字货币芯片卡进行数字货币支付的方法和系统作进一步详细说明。

[0303] 应用场景总览

[0304] 如下示出了本发明实施方式的使用数字货币芯片卡进行离线支付的应用场景,该应用场景包括:

[0305] 付款用户在其持有的数字货币芯片卡(以下简称D-RMB芯片卡)中存有两个面值为100元的数字货币(以下简称D币),一个面值为50元的D币,即该用户拥有两张100元人民币和一张50元人民币,共计250元人民币。

[0306] 假设该付款用户在购物过程中需要通过POS机支付给商家200元人民币,并且商家的POS机处于脱机状态,交易双方无法在网络环境中完成交易,因此商家在POS机上选择离线支付方式。

[0307] 示例性方法

[0308] 下面结合上述的应用场景,参考图7对本发明示例性实施方式的方法进行介绍。该方法包括:

[0309] 步骤A1:受理终端设备在未与商业银行数字货币系统建立网络连接的情况下,接收交易金额;

[0310] 步骤A2:用户终端设备通过近距离无线连接方式从受理终端设备获取交易金额,并将交易信息发送至受理终端设备,交易信息包括数字货币芯片卡信息以及与交易金额等

值的数字货币；

[0311] 步骤A3：受理终端设备与商业银行数字货币系统建立网络连接之后，受理终端设备将交易信息发送至商业银行数字货币系统；

[0312] 步骤A4：商业银行数字货币系统在接收到交易信息后，向中央银行数字货币系统发送变更属主的请求；

[0313] 步骤A5：中央银行数字货币系统在接收到变更属主的请求后，将数字货币的属主变更为受理终端设备对应的商户代码。

[0314] 可选地，近距离无线连接方式包括：NFC、红外线或蓝牙。

[0315] 可选地，受理终端接收付款信息的操作之后，还包括：确认数字货币的属主与数字货币芯片卡相符以及确认交易金额与数字货币的币值相符。

[0316] 可选地，商业银行数字货币系统向中央银行数字货币系统发送变更属主的请求的操作之前，还包括：确认数字货币的合法性、确认数字货币的属主是数字货币芯片卡、确认交易金额与数字货币的币值相符以及确认商户的账户正常使用。

[0317] 可选地，中央银行数字货币系统将数字货币的属主变更为受理终端设备对应的商户代码的操作之前，还包括：确认数字货币的属主是数字货币芯片卡以及确认交易金额与数字货币的币值相符。

[0318] 可选地，数字货币芯片卡包括以下形态：可视蓝牙IC卡形态、IC卡形态、手机-eSE卡形态、手机-安全SD卡形态、手机-SIM卡形态。

[0319] 可选地，受理终端设备是POS收款机或手机刷卡器。

[0320] 可选地，变更待支付的数字货币的属主包括：将权属登记信息中数字货币的钱包地址改为受理终端设备对应对应的商户代码。

[0321] 可选地，将数字货币的属主变更为受理终端设备对应的商户代码的操作之后，还包括：商业银行数字货币系统向用户终端设备和受理终端设备发送用于表示交易成功的提示信息。

[0322] 下面结合具体实施例对本发明进行具体描述，然而值得注意的是该具体实施例仅是为了更好地描述本发明，并不构成对本发明的不当限定。

[0323] 实施例一

[0324] 由于交易双方均处于暂时无法联网的环境中，因此为顺利促成交易，商家可以在受理终端设备(以下简称POS机)上选择离线支付方式，然后输入收款金额200元。

[0325] 首先，付款用户的移动终端(例如手机)通过NFC、红外线或者蓝牙与商家的POS机建立近距离无线通信连接，选取该付款用户的数字货币芯片卡(以下简称D-RMB芯片卡)中交易金额为200元的数字货币(以下简称D币)，并将交易信息发送至该POS机；其中，交该易信息包括D-RMB芯片卡信息以及D币100、D币100'以及D币50，该近距离无线连接方式可以从NFC、红外线或蓝牙这几种近距离无线通信方式中任意选择，并且该数字货币芯片卡可以是可视蓝牙IC卡、普通IC卡、手机内嵌IC卡、手机内置安全SD卡、手机SIM卡或手机云SE形态。

[0326] 该POS机通过调用数字货币系统(以下简称D-RMB系统)的支付插件，获取该交易信息并对该交易信息进行合法性检查。在本发明一实施例中，合法性检查包括：确认数字货币的属主与该D-RMB芯片卡相符、确认付款金额与D币的币值相符。待确认通过之后，POS机打印收款凭条，此时，付款用户与商家的当面交易结束。

[0327] 待该POS机能够接入网络之后,也就是说,该POS机与商业银行D-RMB系统建立网络连接之后,该POS机向商业银行D-RMB系统发送确认重复支付请求,并根据预设的交易规则将交易信息发送至商业银行D-RMB系统。

[0328] 在接收到上述信息后,商业银行D-RMB系统根据预设的交易规则解读上述信息,并确认上述信息的合法性。具体来说,确认合法性包括:D_{币100}、D_{币100'}以及D_{币50}的合法性以及D_币的属主与该D-RMB芯片卡相符、确认商家的银行账号可用等。待确认通过之后,商业银行D-RMB系统根据预设的安全协议将交易涉及的相关信息向中央银行D-RMB系统发送变更交易的D_币的属主的请求。

[0329] 中央银行D-RMB系统在收到支付请求之后,通过解读该交易规则及相关信息,并且确认这些信息的合法性。

[0330] 在本发明一实施例中,确认合法性包括:D_{币100}、D_{币100'}、D_{币50}的合法性,D_币的属主是否为该存款用户的D-RMB芯片卡等。待确认通过之后,中央银行D-RMB系统的登记中心就更改D_{币100}、D_{币100'}、D_{币50}的属主,即将付款用户在权属登记信息中D-RMB芯片卡的钱包地址改为商户的商业银行代码,并且记录本次交易流水。在本发明一实施例中,D-RMB芯片卡所对应的钱包地址包括该数字货币芯片卡的卡号的哈希值。

[0331] 最后,商业银行D-RMB系统向该商家的POS机发送用于表示交易成功的提示信息,并在该商家的账户内增加相应金额(250元)。

[0332] 实施例二

[0333] 在本发明的实施例中使用数字货币芯片卡进行离线支付的方法是商家的POS机自动将D_币转存到商家收款账户。

[0334] 具体来说,付款用户的移动终端通过近距离无线连接方式(NFC、红外线或蓝牙)与商家的POS机建立通信连接,选取账户中金额为200元的D_{币100}、D_{币100'}、D_{币50}发送至该POS机;待POS机接收D_币之后,对接收的D_币进行合法性检查。在本发明一实施例中,该POS机需校验D_币金额是否等值。在校验通过之后当面交易结束,并打印收款凭条。

[0335] 待POS机能够接入网络后,根据预设的交易规则将交易信息、收到D-RMB芯片卡信息和D_币以及商家的银行账号等信息发送至商业银行D-RMB系统。

[0336] 商业银行D-RMB系统解读该交易规则及相关信息,并对这些信息进行合法性确认,然后商业银行D-RMB系统的银行库就收D_{币100}、D_{币100'}、D_{币50},并将这些信息发送至中央银行D-RMB系统。

[0337] 中央银行D-RMB系统通过解读交易规则及相关信息,并确认这些信息合法性。在本发明一实施例中,确认合法性包括:D_币属主是该D-RMB芯片卡,交易金额与D_币的币值相符等。待确认之后,中央银行D-RMB系统的登记中心就更改D_{币100}、D_{币100'}、D_{币50}的属主,即将在权属登记信息中D-RMB芯片卡的钱包地址改为该POS机对应的商家代码,并且记录本次交易流水。在本发明一实施例中,D-RMB芯片卡所对应的钱包地址包括该数字货币芯片卡的卡号的哈希值。

[0338] 最后,商业银行D-RMB系统向该商家的银行账号增加相应金额,反馈相关信息,并且该POS机打印凭条。

[0339] 如图8所示,为本发明还提供的一种使用数字货币芯片卡进行离线支付的系统结构图,该系统8包括:用户终端设备B1、受理终端设备B2、商业银行数字货币系统B3以及中央

银行数字货币系统B4,其中,

[0340] 受理终端设备B2,用于在未与商业银行数字货币系统B3建立网络连接的情况下,接收交易金额,并且在与商业银行数字货币系统B3建立连接之后,受理终端设备B2将交易信息发送至商业银行数字货币系统B3;

[0341] 用户终端设备B1,通过近距离无线连接方式从受理终端设备B2获取交易金额,并将交易信息发送至受理终端设备B2,交易信息包括数字货币芯片卡信息以及与交易金额等值的数字货币;

[0342] 商业银行数字货币系统B3,用于在接收到交易信息后,向中央银行数字货币系统B4发送变更属主的请求;

[0343] 中央银行数字货币系统B4,用于在接收到变更属主的请求后,将数字货币的属主变更为受理终端设备B2对应的商户代码。

[0344] 可选地,近距离无线连接方式包括:NFC、红外线或蓝牙。

[0345] 可选地,受理终端还用于:确认数字货币的属主与数字货币芯片卡相符以及确认交易金额与数字货币的币值相符。

[0346] 可选地,商业银行数字货币系统B3还用于:确认数字货币的合法性、确认数字货币的属主是付款用户、确认交易金额与数字货币的币值相符以及确认商户的账户正常使用。

[0347] 可选地,中央银行数字货币系统B4还用于:确认数字货币的属主是数字货币芯片卡以及确认交易金额与数字货币的币值相符。

[0348] 可选地,数字货币芯片卡包括以下形态:可视蓝牙IC卡形态、IC卡形态、手机-eSE卡形态、手机-安全SD卡形态、手机-SIM卡形态。

[0349] 可选地,受理终端设备B2是POS收款机或手机刷卡器。

[0350] 可选地,变更待支付的数字货币的属主包括:将权属登记信息中数字货币的钱包地址改为受理终端设备B2对应该商户代码。

[0351] 可选地,商业银行数字货币系统B3还用于:向用户终端设备B1和受理终端设备B2发送用于表示交易成功的提示信息。

[0352] 由于本发明提供的使用数字货币芯片卡进行离线支付的系统是上述方法对应的装置,故在此不再赘述。

[0353] 通过本发明提供的使用数字货币芯片卡进行离线支付的方法及系统,由于货币本身的数字化,因此不依赖任何银行账户和单一网络,不仅在保证支付安全的情况下,能够有效提升了消费者在消费过程中的支付体验。

[0354] 从便捷性上来讲,以卡基作为终端载体方案(以下简称“卡基方案”)系统部署便利,用户操作便捷性好、容易推广。

[0355] 与市场其他代替纸币的货币系统相比,D-RMB初步具有便捷性好、安全性高等特点,便捷性表现在以下方面:

[0356] 在发行方式上,D-RMB为货币本身的数字化,不依赖任何银行账户和单一网络;

[0357] 在存储方式上,D-RMB的存储介质可以是手机,也可以是卡、磁盘、计算机等电子设备,为用户提供了多种选择。尤其是以手机为载体的D-RMB可以充分利用手机的键盘、显示、定位、存储、计算、通信等功能,还可二次开发,大大扩充支付场景和便捷性;

[0358] 在支付方式上,既可提供类似于纸币的当面付交易,也可提供类似于电子支付系

统的网络远程支付交易,即可支持联机、也可支持脱机交易,方式便捷、灵活;

[0359] 在交易速度上,付款速度比联机刷卡支付方式有很大提高。非常适于小额快速支付;

[0360] 在使用习惯上,既可兼容原有的刷卡支付方式,也可提供面对面的数字货币支付,同时还可提供电子化的交易记录,便于理财统计,用户可接受度高。

[0361] 安全性表现在以下方面:

[0362] 与其他数字货币系统相比,D-RMB数字货币是由现金数值转换而来的一系列电子加密序列数,通过这些加密序列数的转移来完成支付交易。币本身的安全性由密码算法来保护,可有效保障货币信息的机密性和完整性,安全性高;

[0363] D-RMB数字货币载体的安全性在移动终端利用芯片技术、在后台云端利用可信技术,实现端到端的安全;

[0364] D-RMB数字货币交易系统的安全性一方面依赖于传统的电子支付系统安全技术,同时后台利用强大的D-RMB云计算系统,进一步保障了交易安全;

[0365] 在用户隐私保护方面,通过“前台自愿、后台实名”的方式,既保证了用户隐私,又规避了非法交易的风险。

[0366] 以上所述的具体实施例,对本发明的目的、技术方案和有益效果进行了进一步详细说明,所应理解的是,以上所述仅为本发明的具体实施例而已,并不用于限定本发明的保护范围,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

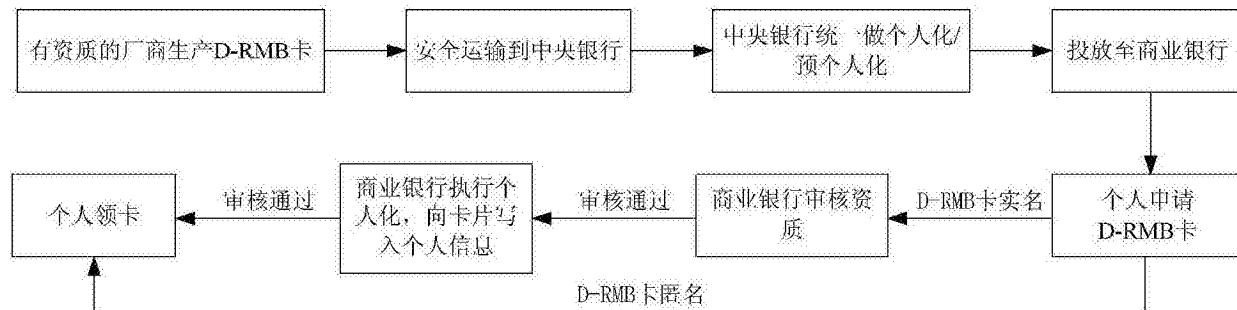


图1

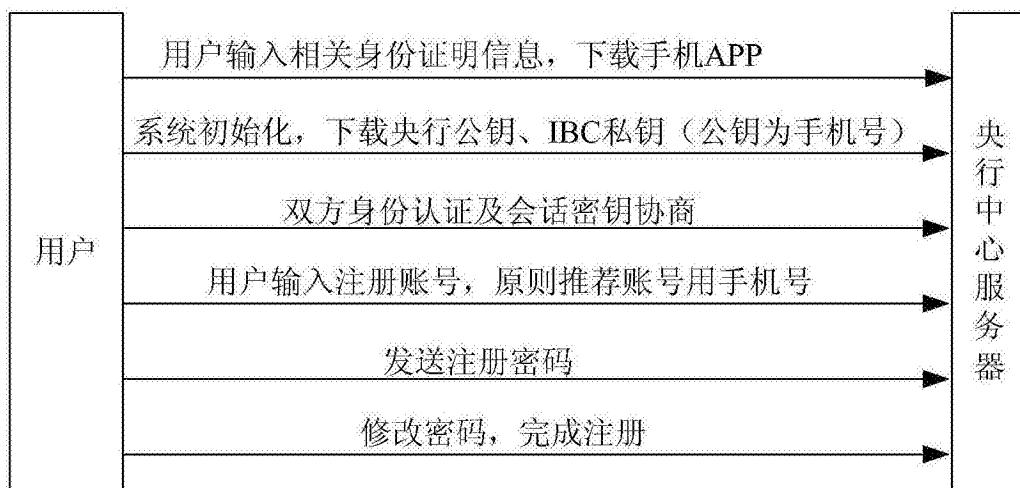


图2

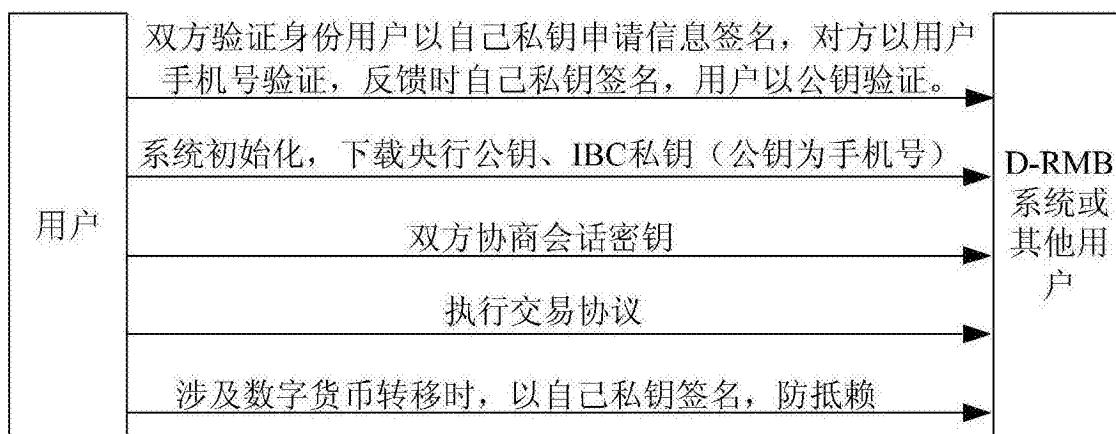


图3

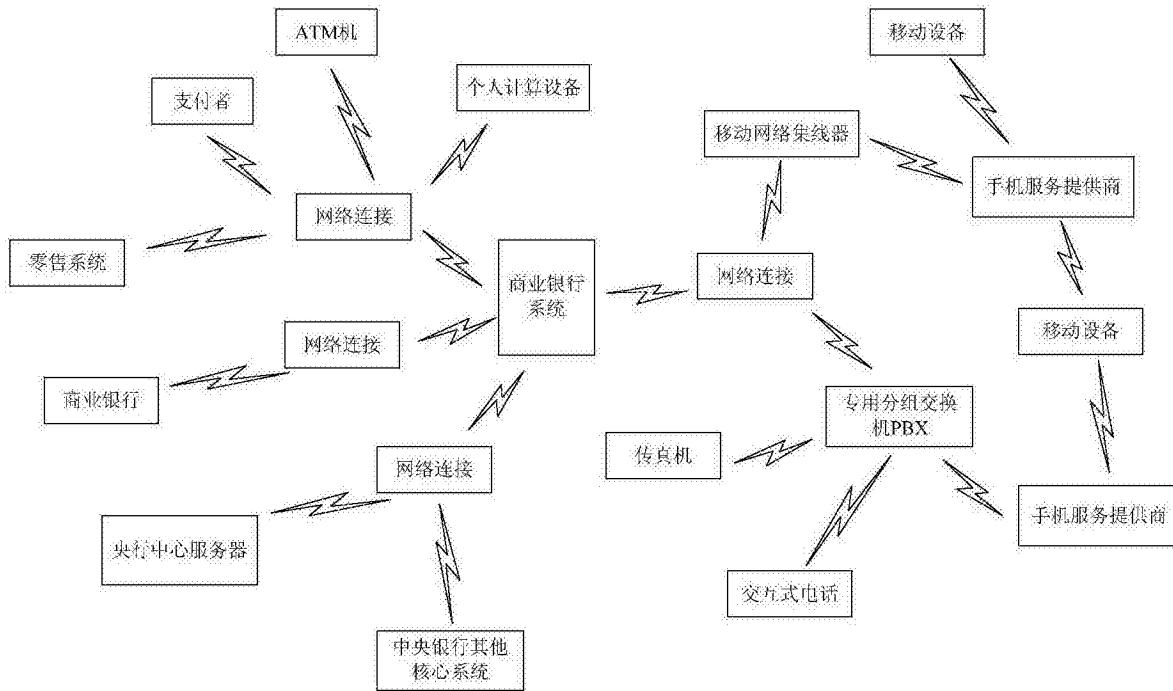


图4

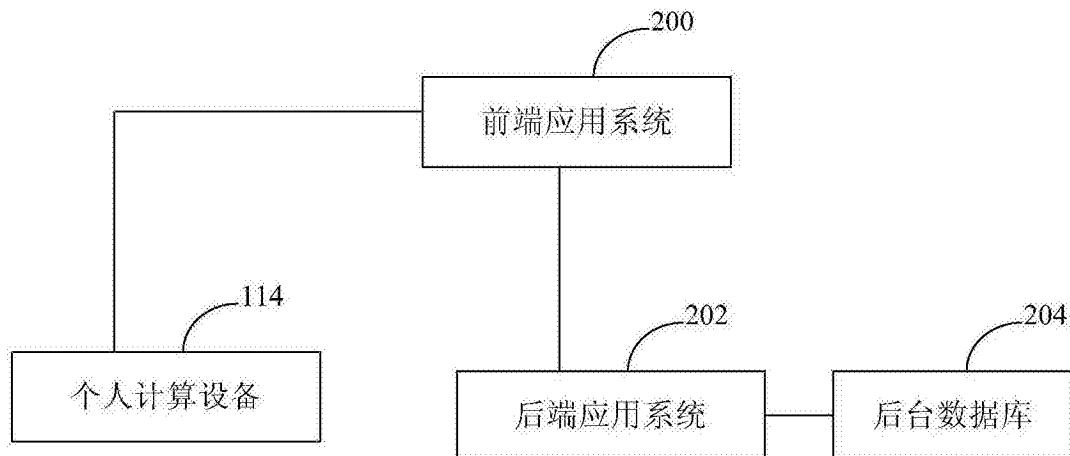


图5

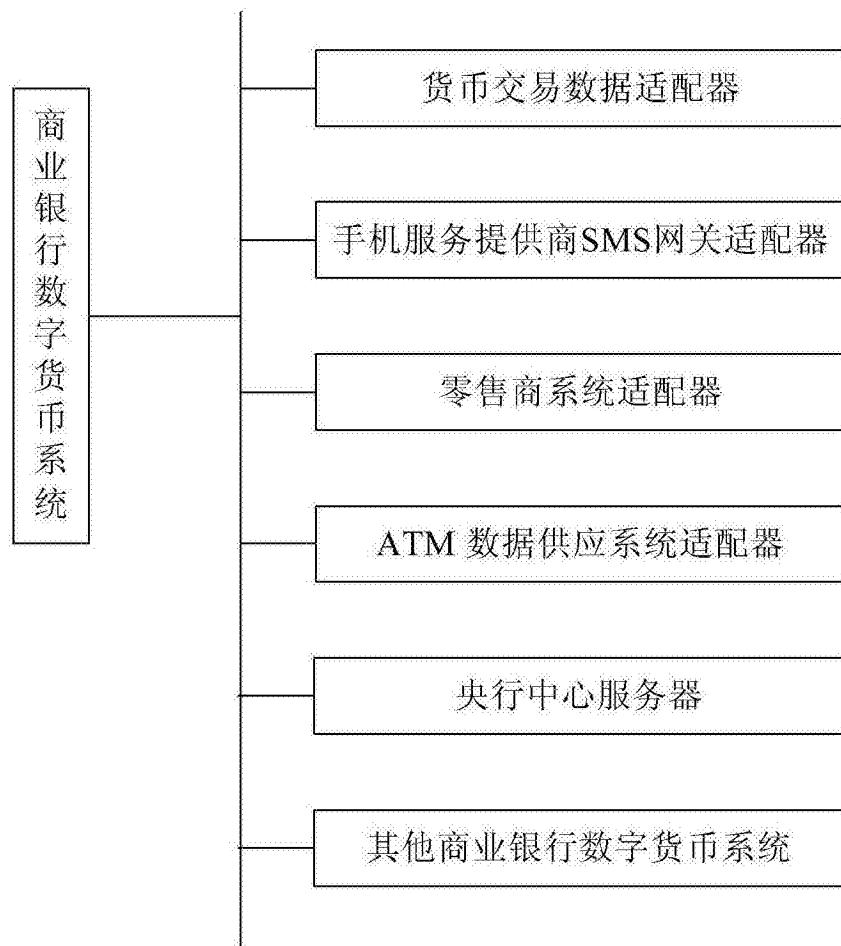


图6

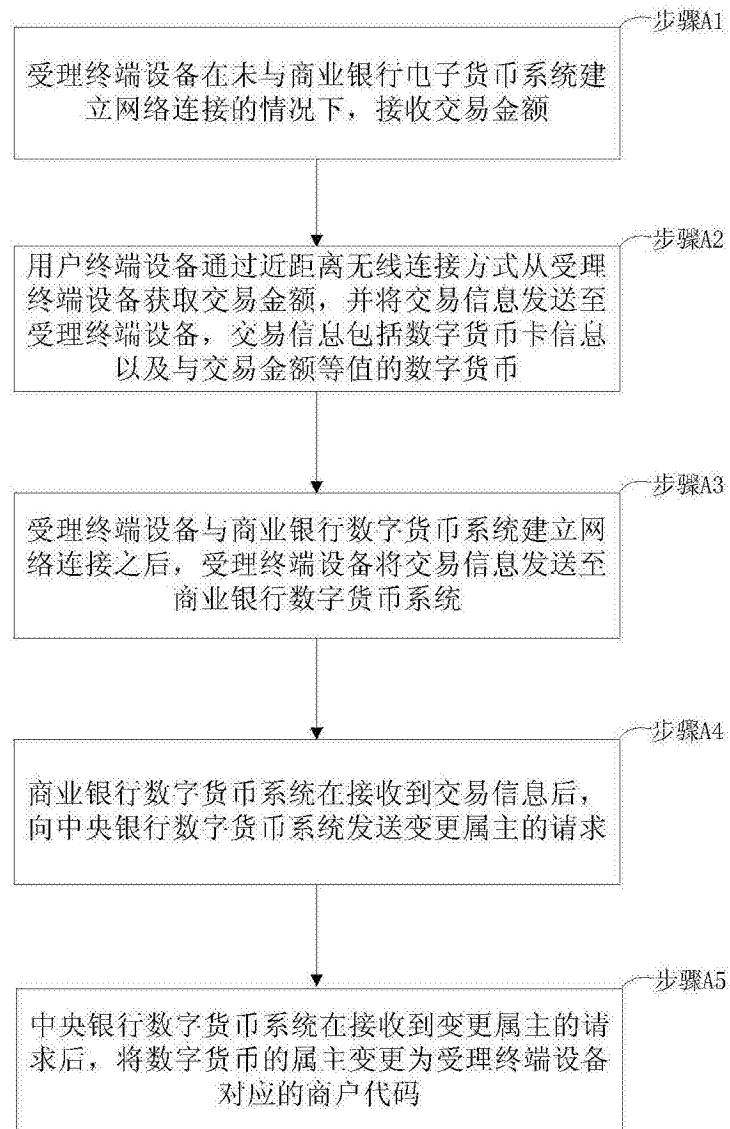


图7

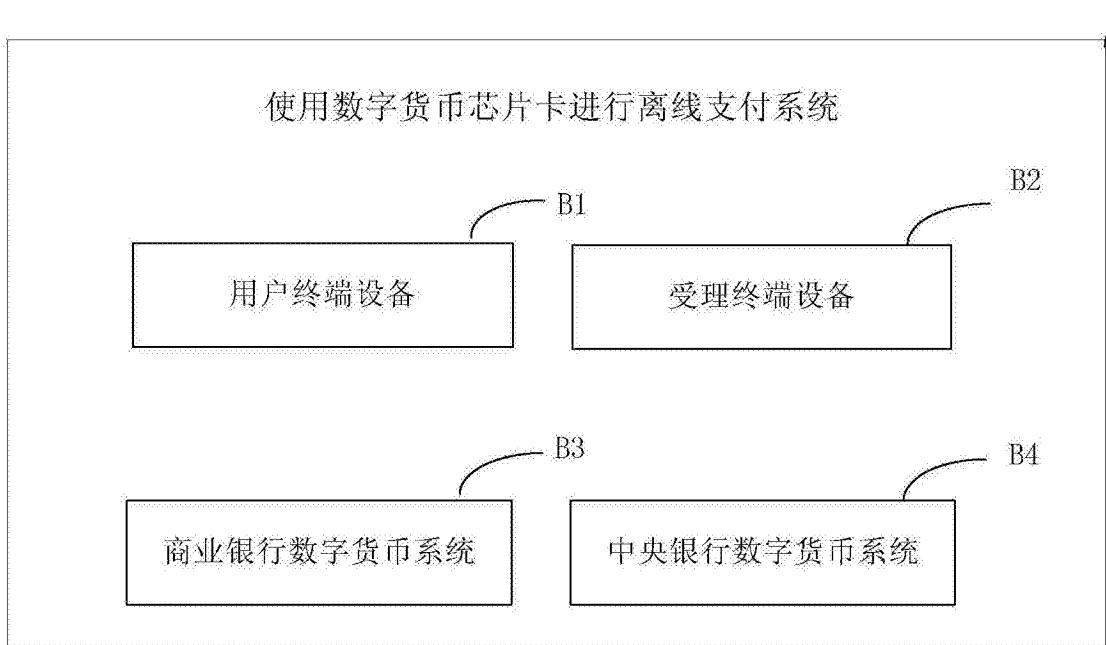


图8