(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 107230049 A
(43)申请公布日 2017.10.03

(21)申请号 201610177297.8

(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责任公司 11219
代理人 张一军 姜劲

(51)Int.Cl.
G06Q 20/06(2012.01)
G06Q 20/10(2012.01)
G06Q 20/36(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
G06Q 40/02(2012.01)

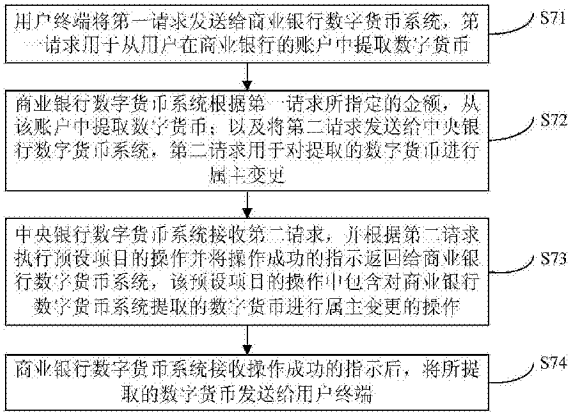
权利要求书2页 说明书14页 附图4页

(54)发明名称

提供数字货币的方法和系统

(57)摘要

本发明提供一种提供数字货币的方法和系统，通过使用用户终端设备来提取数字货币，可以灵活方便地获取数字货币。该方法包括：用户终端将第一请求发送给商业银行数字货币系统；商业银行数字货币系统根据第一请求所指定的金额，从账户中提取数字货币；以及将第二请求发送给中央银行数字货币系统；中央银行数字货币系统接收第二请求，并根据第二请求执行预设项目的操作并将操作成功的指示返回给商业银行数字货币系统，预设项目的操作中包含对商业银行数字货币系统提取的数字货币进行属主变更的操作；商业银行数字货币系统接收操作成功的指示后，将所提取的数字货币发送给用户终端。



CN 107230049 A

1.一种提供数字货币的方法，其特征在于，包括：

用户终端将第一请求发送给商业银行数字货币系统，所述第一请求用于从用户在商业银行的账户中提取数字货币；

所述商业银行数字货币系统根据所述第一请求所指定的金额，从所述账户中提取数字货币；以及将第二请求发送给中央银行数字货币系统，所述第二请求用于对提取的所述数字货币进行属主变更；

所述中央银行数字货币系统接收所述第二请求，并根据所述第二请求执行预设项目的操作并将操作成功的指示返回给所述商业银行数字货币系统，所述预设项目的操作中包含对所述商业银行数字货币系统提取的数字货币进行属主变更的操作；

所述商业银行数字货币系统接收所述操作成功的指示后，将所提取的数字货币发送给所述用户终端。

2.根据权利要求1所述的方法，其特征在于，所述第一请求包括：商业银行的名称、所述账户对应的银行账号及密码、需提取数字货币的金额；

并且，所述商业银行数字货币系统从所述账户中提取数字货币之前，还包括：

所述商业银行数字货币系统确认所述账户对应的银行账号及密码正确、确认所述账户的余额不小于所述需提取数字货币的金额、以及确认所述商业银行数字货币系统中的数字货币余额不小于所述需提取数字货币的金额。

3.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根据所述第二请求执行预设项目的操作之前，还包括：

所述中央银行数字货币系统确认所提取的数字货币的属主为所述商业银行。

4.根据权利要求1所述的方法，其特征在于，所述属主变更的操作包括：

将所述商业银行数字货币系统提取的数字货币的属主由所述商业银行修改为用户的钱包地址，其中，所述钱包地址为公钥，且所述公钥为哈希码。

5.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将所提取的数字货币发送给所述用户终端之后，还包括：

所述商业银行数字货币系统向用户终端发送交易成功的提示信息。

6.根据权利要求1所述的方法，其特征在于，所述数字货币为字符串；所述用户终端为手机，且所述用户终端的标识符为手机号码。

7.一种提供数字货币的系统，其特征在于，包括商业银行数字货币系统和中央银行数字货币系统，其中，

所述商业银行数字货币系统用于接收用户终端发来的第一请求，并根据所述第一请求所指定的金额，从所述账户中提取数字货币；以及将第二请求发送给中央银行数字货币系统；并且在接收到所述中央银行数字货币系统发来的所述操作成功的指示后，将所提取的数字货币发送给所述用户终端；

所述中央银行数字货币系统用于接收所述第二请求，并根据所述第二请求执行预设项目的操作并将操作成功的指示返回给所述商业银行数字货币系统，所述预设项目的操作中包含对所述商业银行数字货币系统提取的数字货币进行属主变更的操作；

其中，所述第一请求用于从用户在商业银行的账户中提取数字货币；

所述第二请求用于对提取的所述数字货币进行属主变更。

8.根据权利要求7所述的提供数字货币的系统，其特征在于，所述第一请求包括：商业银行的名称、所述账户对应的银行账号及密码、需提取数字货币的金额；

并且，所述商业银行数字货币系统在从所述账户中提取数字货币之前，还用于：所述商业银行数字货币系统确认所述账户对应的银行账号及密码正确、确认所述账户的余额不小于所述需提取数字货币的金额、以及确认所述商业银行数字货币系统中的数字货币余额不小于所述需提取数字货币的金额。

9.根据权利要求7所述的提供数字货币的系统，其特征在于，所述中央银行数字货币系统在根据所述第二请求执行预设项目的操作之前，还用于：

所述中央银行数字货币系统确认所提取的数字货币的属主为所述商业银行。

10.根据权利要求7所述的提供数字货币的系统，其特征在于，所述属主变更的操作包括：

将所述商业银行数字货币系统提取的数字货币的属主由所述商业银行修改为用户的钱包地址，其中，所述钱包地址为公钥，且所述公钥为哈希码。

11.根据权利要求7所述的提供数字货币的系统，其特征在于，所述商业银行数字货币系统在将所提取的数字货币发送给所述用户终端之后，还用于：

所述商业银行数字货币系统向用户终端发送交易成功的提示信息。

12.根据权利要求7所述的提供数字货币的系统，其特征在于，所述数字货币为字符串；所述用户终端为手机，且所述用户终端的标识符为手机号码。

提供数字货币的方法和系统

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，特别地涉及一种提供数字货币的方法和系统。

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，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D-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] 数字货币以电子计算机技术为依托进行储存、支付和流通，可广泛应用于生产、交换、分配和消费等多个领域。由于数字货币集金融储蓄、信贷和非现金结算等多种功能为一体，故而具有使用简便、安全、迅速、可靠的特征。然而，现阶段数字货币的使用通常以银行卡(磁卡、智能卡)为媒体。而以银行卡为媒体，即限制了必须要能识别和操作银行卡才能使用数字货币，这极大地限制了数字货币的广泛使用和流通。

发明内容

[0017] 有鉴于此，本发明提供一种提供数字货币的方法和系统，主要指通过移动终端设备来提取数字货币的方法和系统，以解决现有技术中的上述种种不足之处。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。

[0018] 为实现上述目的，根据本发明的一个方面，提供了一种提供数字货币的方法。

[0019] 本发明的一种提供数字货币的方法包括：用户终端将第一请求发送给商业银行数字货币系统，所述第一请求用于从用户在商业银行的账户中提取数字货币；所述商业银行数字货币系统根据所述第一请求所指定的金额，从所述账户中提取数字货币；以及将第二请求发送给中央银行数字货币系统，所述第二请求用于对提取的所述数字货币进行属主变更；所述中央银行数字货币系统接收所述第二请求，并根据所述第二请求执行预设项目的操作并将操作成功的指示返回给所述商业银行数字货币系统，所述预设项目的操作中包含对所述商业银行数字货币系统提取的数字货币进行属主变更的操作；所述商业银行数字货币系统接收所述操作成功的指示后，将所提取的数字货币发送给所述用户终端。

[0020] 可选地，所述第一请求包括：商业银行的名称、所述账户对应的银行账号及密码、需提取数字货币的金额；并且，所述商业银行数字货币系统从所述账户中提取数字货币之前，还包括：所述商业银行数字货币系统确认所述账户对应的银行账号及密码正确、确认所述账户的余额不小于所述需提取数字货币的金额、以及确认所述商业银行数字货币系统中的数字货币余额不小于所述需提取数字货币的金额。

[0021] 可选地，所述中央银行数字货币系统根据所述第二请求执行预设项目的操作之前，还包括：所述中央银行数字货币系统确认所提取的数字货币的属主为所述商业银行。

[0022] 可选地，所述属主变更的操作包括：将所述商业银行数字货币系统提取的数字货币的属主由所述商业银行修改为用户的钱包地址，其中，所述钱包地址为公钥，且所述公钥为哈希码。

[0023] 可选地，所述商业银行数字货币系统将所提取的数字货币发送给所述用户终端之后，还包括：所述商业银行数字货币系统向用户终端发送交易成功的提示信息。

[0024] 可选地，所述数字货币为字符串；所述用户终端为手机，且所述用户终端的标识符为手机号码。

[0025] 根据本发明的另一方面，提供了一种提供数字货币的系统。

[0026] 本发明的一种提供数字货币的系统，包括商业银行数字货币系统和中央银行数字货币系统，其中，所述商业银行数字货币系统用于接收用户终端发来的第一请求，并根据所述第一请求所指定的金额，从所述账户中提取数字货币；以及将第二请求发送给中央银行数字货币系统；并且在接收到所述中央银行数字货币系统发来的所述操作成功的指示后，将所提取的数字货币发送给所述用户终端；所述中央银行数字货币系统用于接收所述第二请求，并根据所述第二请求执行预设项目的操作并将操作成功的指示返回给所述商业银行数字货币系统，所述预设项目的操作中包含对所述商业银行数字货币系统提取的数字货币进行属主变更的操作；其中，所述第一请求用于从用户在商业银行的账户中提取数字货币；所述第二请求用于对提取的所述数字货币进行属主变更。

[0027] 可选地，所述第一请求包括：商业银行的名称、所述账户对应的银行账号及密码、需提取数字货币的金额；并且，所述商业银行数字货币系统在从所述账户中提取数字货币之前，还用于：所述商业银行数字货币系统确认所述账户对应的银行账号及密码正确、确认所述账户的余额不小于所述需提取数字货币的金额、以及确认所述商业银行数字货币系统中的数字货币余额不小于所述需提取数字货币的金额。

[0028] 可选地，所述中央银行数字货币系统在根据所述第二请求执行预设项目的操作之前，还用于：所述中央银行数字货币系统确认所提取的数字货币的属主为所述商业银行。

[0029] 可选地，所述属主变更的操作包括：将所述商业银行数字货币系统提取的数字货币的属主由所述商业银行修改为用户的钱包地址，其中，所述钱包地址为公钥，且所述公钥为哈希码。

[0030] 可选地，所述商业银行数字货币系统在将所提取的数字货币发送给所述用户终端之后，还用于：所述商业银行数字货币系统向用户终端发送交易成功的提示信息。

[0031] 可选地，所述数字货币为字符串；所述用户终端为手机，且所述用户终端的标识符为手机号码。

[0032] 根据本发明的技术方案，通过使用用户终端设备来提取数字货币，从而可以灵活方便地获取数字货币；通过在各个环节进行多次验证，并且根据交易规则组织相关信息并发送，从而可以增强交易的安全性；通过中央银行数字货币系统进行数字货币的属主变更，可以实现由中央银行统一记录数字货币的交易情况，从而实现数字货币的安全和统一管理。

附图说明

[0033] 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；

[0034] 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；

[0035] 图3是与本发明实施方式有关的D-RMB交易过程的示意图；

[0036] 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；

[0037] 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；

[0038] 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；

[0039] 图7是根据本发明实施方式的提供数字货币的方法的主要步骤示意图；

[0040] 图8是根据本发明实施方式的提供数字货币的系统的主要组成部分示意图。

具体实施方式

[0041] 以下结合附图对本发明的示范性实施例做出说明，其中包括本发明实施例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例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。

[0042] 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“$D_{币}$”。

[0043] 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：

[0044] 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。

[0045] 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。

[0046] 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。

[0047] 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。

[0048] 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。

[0049] 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。

[0050] 为方便后续的描述，对以下符号约定：

[0051] 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。

[0052] 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。

[0053] $D_{银行}$：指银行在央行中心系统开设的准备金账户，作记账用。

[0054] $D_{币}$: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。

[0055] $D_{币100}$: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。

[0056] $B_{账号}$:用户所在开户行的银行账号。

[0057] 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。

[0058] 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。

[0059] 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。

[0060] 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。

[0061] 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:

[0062] 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。

[0063] 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。

[0064] 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。

[0065] 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。

[0066] 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:

[0067] (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。

[0068] (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。

[0069] 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。

[0070] (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。

[0071] (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。

[0072] 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)。

[0073] 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。

[0074] 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”)。

[0075] (1)D-RMB芯片卡的生产

[0076] 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。

[0077] (2)D-RMB芯片卡的个性化

[0078] 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。

[0079] (3)D-RMB芯片卡的发行

[0080] 系统可支持实名制发卡和匿名发卡。

[0081] 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。

[0082] 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。

[0083] 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。

[0084] 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。

[0085] 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。

[0086] 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。

[0087] 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。

[0088] 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。

[0089] 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。

[0090] 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。

[0091] 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。

[0092] 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:

[0093] 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。

[0094] 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H(手机号1)改为H(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。

[0095] 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。

[0096] 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。

[0097] 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。

[0098] 总的说来，D-RMB体系的核心要素为一种币、两类库、三个中心：

[0099] 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。

[0100] 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。

[0101] 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。

[0102] 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。

[0103] 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。

[0104] 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。

[0105] 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。

[0106] 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。

[0107] 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。

[0108] 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。

[0109] 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。

[0110] 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。

[0111] 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。

[0112] 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。

[0113] 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。

[0114] 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。

[0115] 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。

[0116] 以下将以用户手机作为终端方式，以手机号作为身份标识，对操作D-RMB的各种业务流程加以阐述，主要包括客户端下载登录、提取、支付、存款及兑现等流程，进行面对面交易方式来阐述。用户的客户端登录、提取、兑现流程要求用户必须在在线状态下完成，而支付过程可以分为在线支付和离线支付，于是形成多个场景状态及其对应的流程，各个流程要达到的目的是由一系列操作步骤来实现。除了手机以外，目前以及将来可能出现的其他智能终端都可以作为D-RMB的载体并执行各种业务流程。

[0117] 以下分别对流程的概要(以下的“流程说明”)和场景状态(以下的“场景说明”)以

及在该场景中实现该流程的步骤(以下的“步骤说明”)一一加以描述。

[0118] 关于用户客户端下载登录,按以下流程执行:

[0119] 流程说明:用户通过手机下载由商业银行提供的APP安装程序登录D-RMB系统过程。

[0120] 场景说明:有资质的商业银行(如工商银行)连接CA认证中心、IBC认证中心和登记中心,对用户提供数字货币服务。用户通过手机下载由商业银行提供的APP安装程序登录商业银行D-RMB系统。

[0121] 步骤说明:

[0122] 步骤1.用户以手机登录商行(如中国工商银行)D-RMB系统页面,下载由商业银行提供的手机APP安装程序,对于已有账号(IBC认证中心)的用户,可以直接登录;对于新的用户,需要首先进行账户初始化操作;

[0123] 步骤2.初始化:在页面录入相关信息(如姓名、住址、电子邮件地址、手机号、身份证号、注册账号即手机号等),点击发送;

[0124] 步骤3.商业银行:连接IBC认证中心,为该用户创建D-RMB数字货币系统唯一账号,并在IBC中心验证其唯一性。个人用户可采用手机号,生成用户初始登录密码并发送给用户手机;IBC中心根据手机号产生用户的私钥,公钥为用户手机号,以公钥作为账号进行交易流转;

[0125] 步骤4.用户手机端:接收到初始登录密码后激活账户,下载用户私钥和央行公钥到手机安全保护区,通过再次登录手机APP来修改登录密码,完成初始化。

[0126] 用户如果申请换手机卡,则密钥可提前预植在卡片SE区。

[0127] 以下再对本发明实施方式中的提供数字货币的方法和系统作进一步详细说明。

[0128] 图7是根据本发明实施方式的提供数字货币的方法的主要步骤示意图。如图7所示,本发明的提供数字货币的方法主要包括如下的步骤S71至步骤S74。

[0129] 步骤S71:用户终端将第一请求发送给商业银行数字货币系统,第一请求用于从用户在商业银行的账户中提取数字货币;

[0130] 步骤S72:商业银行数字货币系统根据第一请求所指定的金额,从该账户中提取数字货币;以及将第二请求发送给中央银行数字货币系统,第二请求用于对提取的数字货币进行属主变更;

[0131] 步骤S73:中央银行数字货币系统接收第二请求,并根据第二请求执行预设项目的操作并将操作成功的指示返回给商业银行数字货币系统,该预设项目的操作中包含对商业银行数字货币系统提取的数字货币进行属主变更的操作;

[0132] 步骤S74:商业银行数字货币系统接收操作成功的指示后,将所提取的数字货币发送给用户终端。

[0133] 根据本发明的技术方案,第一请求可以包括:商业银行的名称、所述账户对应的银行账号及密码、需提取数字货币的金额。并且,步骤S72中,商业银行数字货币系统从该账户中提取数字货币之前,还可以包括:商业银行数字货币系统确认所述账户对应的银行账号及密码正确、确认所述账户的余额不小于需提取数字货币的金额、以及确认商业银行数字货币系统中的数字货币余额不小于需提取数字货币的金额。商业银行数字货币系统在对以上信息进行确认时,是通过对第一请求进行第一验证来实现的,其中,第一验证包括校验该

账户对应的银行账号及密码的正确性、判断该账户的余额是否不小于需提取数字货币的金额、以及判断商业银行数字货币系统中的数字货币余额是否不小于需提取数字货币的金额；当第一验证通过时，则执行商业银行数字货币系统从该账户中提取数字货币。此处，商业银行数字货币系统在提取数字货币时，是通过在数字货币系统中对提取的数字货币进行记录的方式进行的。

[0134] 商业银行数字货币系统在第一验证通过后，从该商业银行的该账户名下进行扣款，并在提取了数字货币后生成第二请求。在生成第二请求时，可以根据预先制定的交易规则将用户终端的标识符与所提取的数字货币的标识码进行组织以生成第二请求。另外，根据用户交易内容的不同，交易规则也会进行相应地变化，且第二请求的具体内容也会发生相应的变化。另外，根据交易的安全需要，交易规则中还可以包括对交易信息进行哈希运算等以实现加密、以及以用户终端标识符的私钥对哈希运算后的字符串进行签名以实现进一步的加密处理等。

[0135] 另外，中央银行数字货币系统在根据第二请求执行预设项目的操作之前，为了系统的安全，还需要确认所提取的数字货币的属主为该商业银行。中央银行数字货币系统在进行数字货币的属主信息确认时，可以通过对第二请求进行第二验证来实现，其中，第二验证主要包括：验证所提取的数字货币的属主是否为该商业银行；如果是，则第二验证通过，中央银行数字货币系统根据第二请求执行预设项目的操作。

[0136] 预设项目的操作中包含的对商业银行数字货币系统提取的数字货币进行属主变更的操作具体可以是：将商业银行数字货币系统提取的数字货币的属主由商业银行修改为用户的钱包地址，其中，钱包地址为公钥，且该公钥可以为哈希码。在本发明中，预设项目的操作是在中央银行数字货币系统的登记中心进行的，在登记中心进行数字货币的属主信息登记时，对应属主信息可记录为公钥哈希，如H(手机号)，以增强匿名性，或者在登记中心中，公钥可以由用户自行设定，用户也可完全用一串无意义码来代表公钥等。

[0137] 并且，预设项目的操作中还可以包括记录相应的交易详情信息。其中，记录的相应的交易详情信息例如包括：此次交易发生的时间、属主变更的时间以及变更前后的属主信息等等，可根据不同的交易内容进行记录，以便日后查询。数字货币的属主即是数字货币的拥有者，当进行数字货币的交易时，需要在中央银行数字货币系统的登记中心将该数字货币对应的字符串的拥有者信息进行更改，并记录下来，以表示该数字货币的属主发生了变更。

[0138] 另外，在商业银行数字货币系统将所提取的数字货币发送给用户终端之后，还可以，由商业银行数字货币系统向用户终端发送交易成功的提示信息，以提示此次交易执行成功。

[0139] 在本发明的技术方案中，数字货币为字符串；用户终端优选为手机，且用户终端的标识符为手机号码。根据实际使用的需要，用户终端也可以包括其他的可联网的移动设备，例如平板电脑等，且用户终端的标识符例如可以是自定义的一串唯一字符串或者电子邮箱地址等等。

[0140] 下面以用户通过手机上安装的数字货币系统的应用程序APP从中国工商银行数字货币系统提取250元的数字货币为例，对本发明的提供数字货币的详细步骤进行说明。

[0141] 步骤1：用户登录手机APP，选择功能“提取数字货币”，选择指定的商业银行，例如

中国工商银行，输入用户账户所对应的银行账号及密码、所需提取数字货币的金额(如250元)等要素，点击“发送”以将该第一请求发送给中国工商银行的商业银行数字货币系统；

[0142] 步骤2：商业银行数字货币系统：验证该第一请求的合法性，如核验银行账号及密码是否正确、该用户账户对应的银行账号即$B_{账号}$余额是否够付(即：$B_{账号}$的余额是否不小于需提取数字货币的金额)、银行库中的数字货币余额$D_{币}$是否够付(即：该商业银行数字货币系统中的数字货币余额是否不小于需提取数字货币的金额)等；在验证通过后，该商业银行数字货币系统将$B_{账号}$的余额扣款250元，并从银行库支取$D_{币100}$，$D_{币100}$’以及$D_{币50}$(即：该商业银行数字货币系统记录该数字货币$D_{币100}$，$D_{币100}$’以及$D_{币50}$对应的字符串)；然后，根据交易规则组织相关信息向中央银行数字货币系统D-RMB系统发送第二请求，此处，相关信息需包括用户终端的标识符(例如：用户的手机号)与所提取的数字货币$D_{币100}$，$D_{币100}$’以及$D_{币50}$对应的字符串；

[0143] 步骤3：中央银行数字货币系统：接收到第二请求后，解读交易规则及相关信息，并验证相关内容的合法性(如支取的数字货币$D_{币100}$，$D_{币100}$’以及$D_{币50}$的属主是否为中国工商银行等)，并在验证通过后，登记中心将执行如下的相关操作：变更$D_{币100}$，$D_{币100}$’以及$D_{币50}$对应的属主信息，亦即，将$D_{币100}$，$D_{币100}$’以及$D_{币50}$的属主由之前绑定的中国工商银行的代码改为用户的钱包地址，即公钥哈希，并记录相应的交易流水详情信息；

[0144] 步骤4：商业银行数字货币系统：将$D_{币100}$，$D_{币100}$’以及$D_{币50}$对应的字符串发送到用户手机，完成内部相应操作，并向用户发送交易成功提示信息。

[0145] 图8是根据本发明实施方式的提供数字货币的系统的主要组成部分示意图。如图8所示，本发明的提供数字货币的系统80主要包括商业银行数字货币系统81和中央银行数字货币系统82两个部分。

[0146] 商业银行数字货币系统81用于接收用户终端发来的第一请求，并根据所述第一请求所指定的金额，从所述账户中提取数字货币；以及将第二请求发送给中央银行数字货币系统；并且在接收到所述中央银行数字货币系统发来的所述操作成功的指示后，将所提取的数字货币发送给所述用户终端；中央银行数字货币系统82用于接收所述第二请求，并根据所述第二请求执行预设项目的操作并将操作成功的指示返回给所述商业银行数字货币系统，所述预设项目的操作中包含对所述商业银行数字货币系统提取的数字货币进行属主变更的操作；其中，所述第一请求用于从用户在商业银行的账户中提取数字货币；所述第二请求用于对提取的所述数字货币进行属主变更。

[0147] 其中，所述第一请求包括：商业银行的名称、所述账户对应的银行账号及密码、需提取数字货币的金额；并且，商业银行数字货币系统81在从所述账户中提取数字货币之前，还可以用于：所述商业银行数字货币系统确认所述账户对应的银行账号及密码正确、确认所述账户的余额不小于所述需提取数字货币的金额、以及确认所述商业银行数字货币系统中的数字货币余额不小于所述需提取数字货币的金额。

[0148] 中央银行数字货币系统82在根据所述第二请求执行预设项目的操作之前，还可以用于：中央银行数字货币系统确认所提取的数字货币的属主为所述商业银行。

[0149] 根据本发明实施例的技术方案，属主变更的操作具体可以包括：将所述商业银行数字货币系统提取的数字货币的属主由所述商业银行修改为用户的钱包地址，其中，所述钱包地址为公钥，且所述公钥为哈希码。

[0150] 商业银行数字货币系统81在将所提取的数字货币发送给所述用户终端之后，还可以用于：商业银行数字货币系统向用户终端发送交易成功的提示信息。

[0151] 本发明中，所述数字货币为字符串；所述用户终端为手机，且所述用户终端的标识符为手机号码。

[0152] 以下对于重复交易检测加以说明。在线交易情况下，D-RMB系统通过D币与用户账号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：

[0153] 表1

[0154]

数字货币名	属主	备注
Pbc100adfk109987766670	138xxxxx 001	D币100
……	……	……
Pbc50cadfk109987766670	137xxxxx 002	D币50

[0155] 用户1(手机号138xxxxx001)在向用户2(手机号138xxxxx002)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138xxxxx001的钱包地址更改为手机号138xxxxx002的钱包地址，如果用户1还想用D币100向其它用户支付，此时其属主已不是用户1，无法完成支付，以此来防止重复支付。

[0156] 如果在D-RMB系统中登记中心权属登记表以公钥哈希代表属主，则登记中心权属登记表可设计如表2：

[0157] 表2

[0158]

数字货币名	属主	备注
Pbc100adfk109987766670	1Xadcfdgdadg	D 币 100 H（138xxxxx001）
……	……	……
Pbc50cadfk109987766670	2xcfdald3xgdf	D 币 50 H（138xxxxx002）

[0159] 假设H(138xxxxx001)值为1Xadcfdgdadg，H(138xxxxx002)值为2xcfdald3xgdf，用户1(手机号138xxxxx001)在向用户2(手机号138xxxxx002)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1Xadcfdgdadg更改为2xcfdald3xgdf，如果用户1还想用D币100向其它用户支付，此时其属主已不是用户1，无法完成支付，以此来防止重复支付。

[0160] 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。

[0161] 同时我们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。

[0162] 根据本发明实施例的技术方案，通过使用用户终端设备来提取数字货币，从而可以灵活方便地获取数字货币；通过在各个环节进行多次验证，并且根据交易规则组织相关

信息并发送，从而可以增强交易的安全性；通过中央银行数字货币系统进行数字货币的属主变更，可以实现由中央银行统一记录数字货币的交易情况，从而实现数字货币的安全和统一管理。

[0163] 从便捷性上来讲，以手机作为终端载体方案(以下简称“手机方案”)提供了更多的实现方式和使用手段，系统部署便利，用户操作便捷性好、更易推广。

[0164] 从安全性上考虑，以手机为D-RMB载体，可采用HCE和TEE方案，从而提供了更大存储空间，不完全依赖硬件厂商，推广更为便利。

[0165] 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：

[0166] 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；

[0167] 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；

[0168] 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；

[0169] 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；

[0170] 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。

[0171] 安全性表现在以下方面：

[0172] 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；

[0173] 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；

[0174] 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；

[0175] 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。

[0176] 上述具体实施方式，并不构成对本发明保护范围的限制。本领域技术人员应该明白的是，取决于设计要求和其他因素，可以发生各种各样的修改、组合、子组合和替代。任何在本发明的精神和原则之内所作的修改、等同替换和改进等，均应包含在本发明保护范围之内。

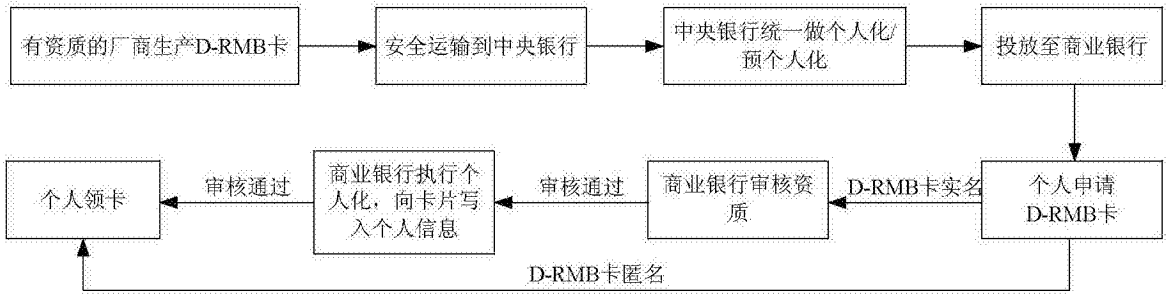

有资质的厂商生产D-RMB卡
安全运输到中央银行
中央银行统一做个人化/预个人化
投放至商业银行
个人申请D-RMB卡
D-RMB卡实名
商业银行审核资质
审核通过
商业银行执行个人化，向卡片写入个人信息
审核通过
个人领卡
D-RMB卡匿名

图1

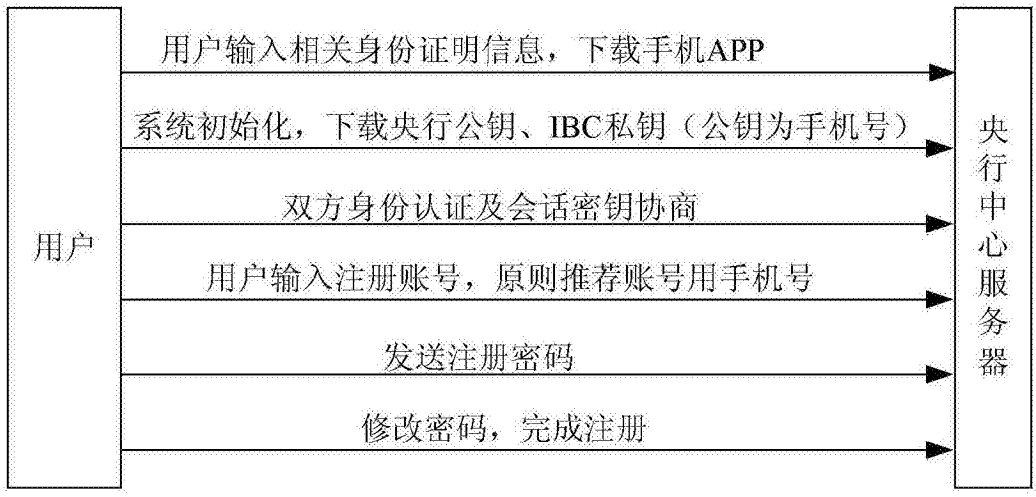

用户
用户输入相关身份证明信息，下载手机APP
系统初始化，下载央行公钥、IBC私钥（公钥为手机号）
双方身份认证及会话密钥协商
用户输入注册账号，原则推荐账号用手机号
发送注册密码
修改密码，完成注册
央行中心服务器

图2

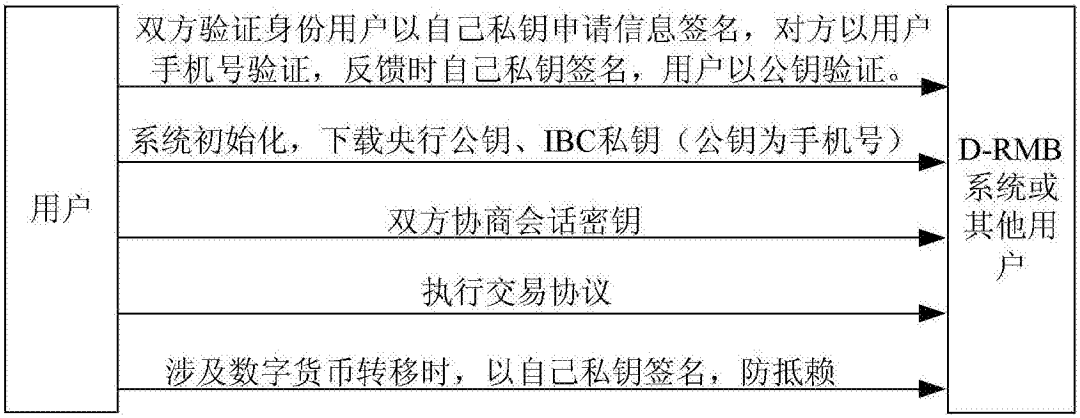

用户
双方验证身份用户以自己私钥申请信息签名，对方以用户手机号验证，反馈时自己私钥签名，用户以公钥验证。
系统初始化，下载央行公钥、IBC私钥（公钥为手机号）
双方协商会话密钥
执行交易协议
涉及数字货币转移时，以自己私钥签名，防抵赖
D-RMB系统或其他用户

图3

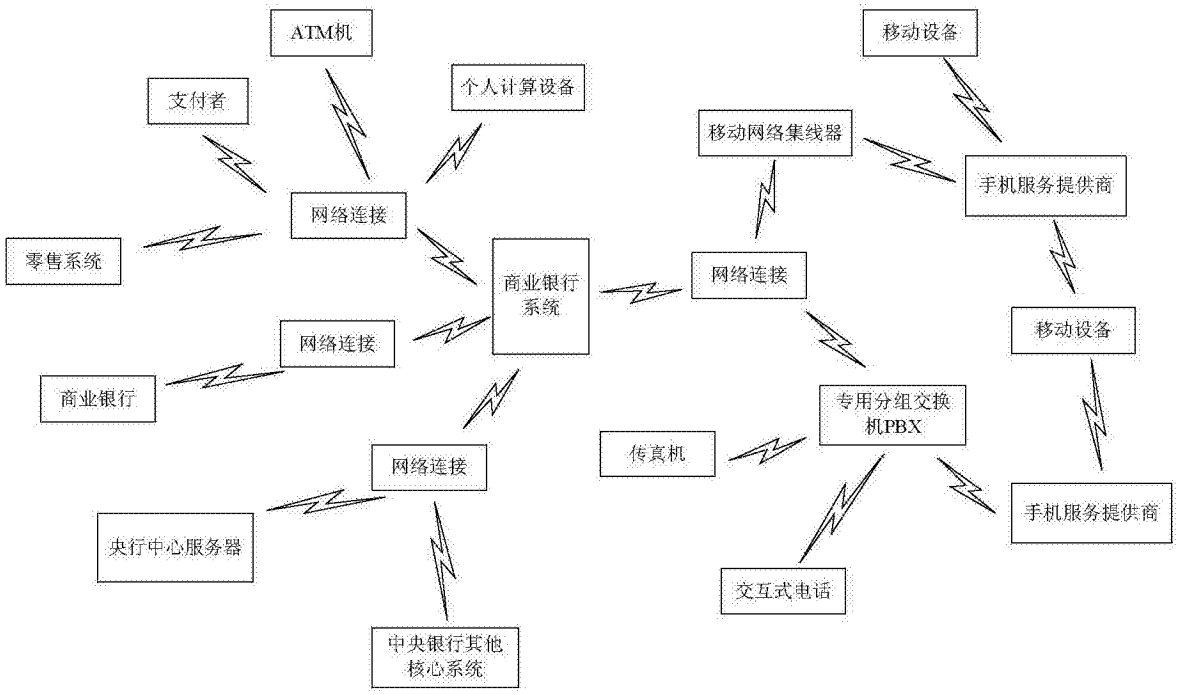

ATM机
支付者
个人计算设备
网络连接
零售系统
商业银行系统
网络连接
商业银行
网络连接
央行中心服务器
中央银行其他核心系统
移动设备
移动网络集线器
手机服务提供商
网络连接
移动设备
专用分组交换机PBX
传真机
手机服务提供商
交互式电话

图4

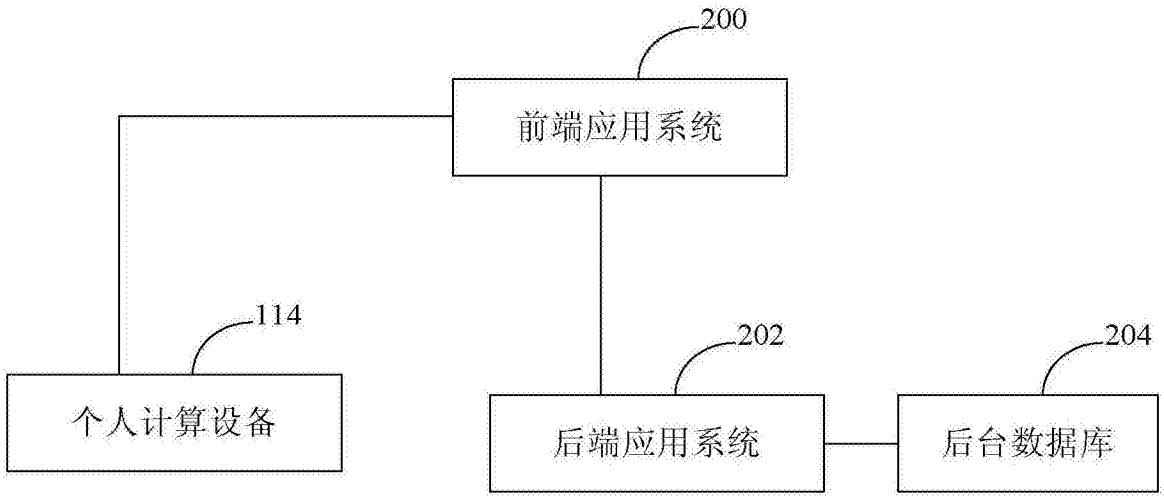

200
前端应用系统
114
个人计算设备
202
后端应用系统
204
后台数据库

图5

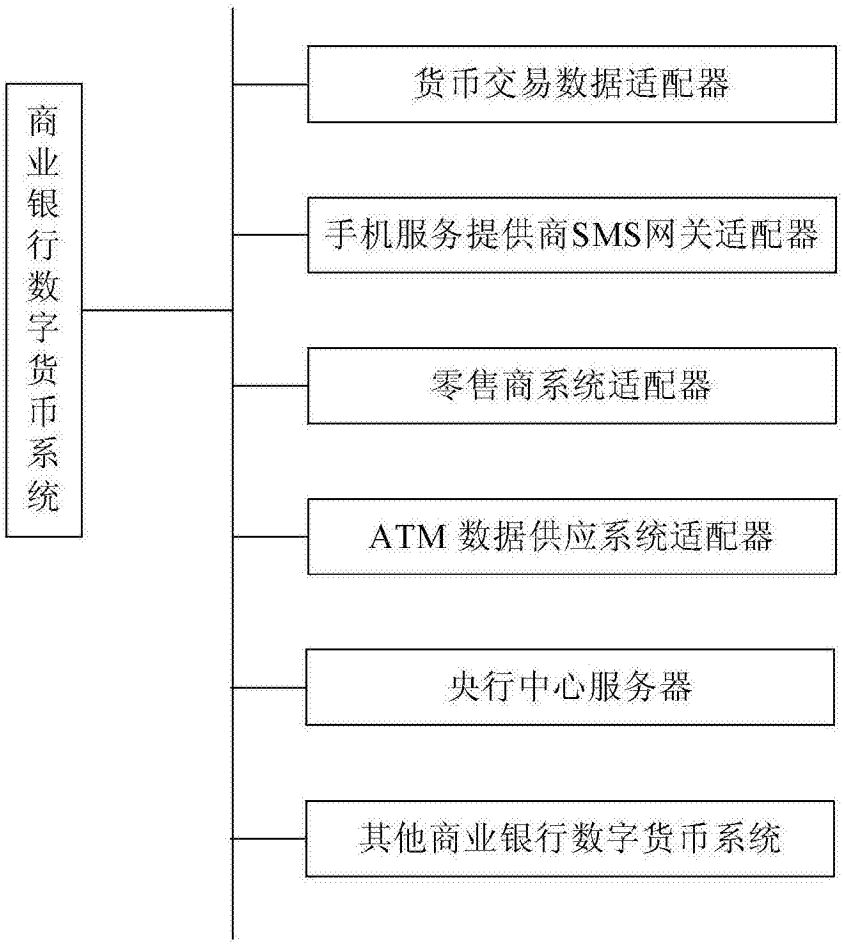

商业银行数字货币系统
货币交易数据适配器
手机服务提供商SMS网关适配器
零售商系统适配器
ATM 数据供应系统适配器
央行中心服务器
其他商业银行数字货币系统

图6

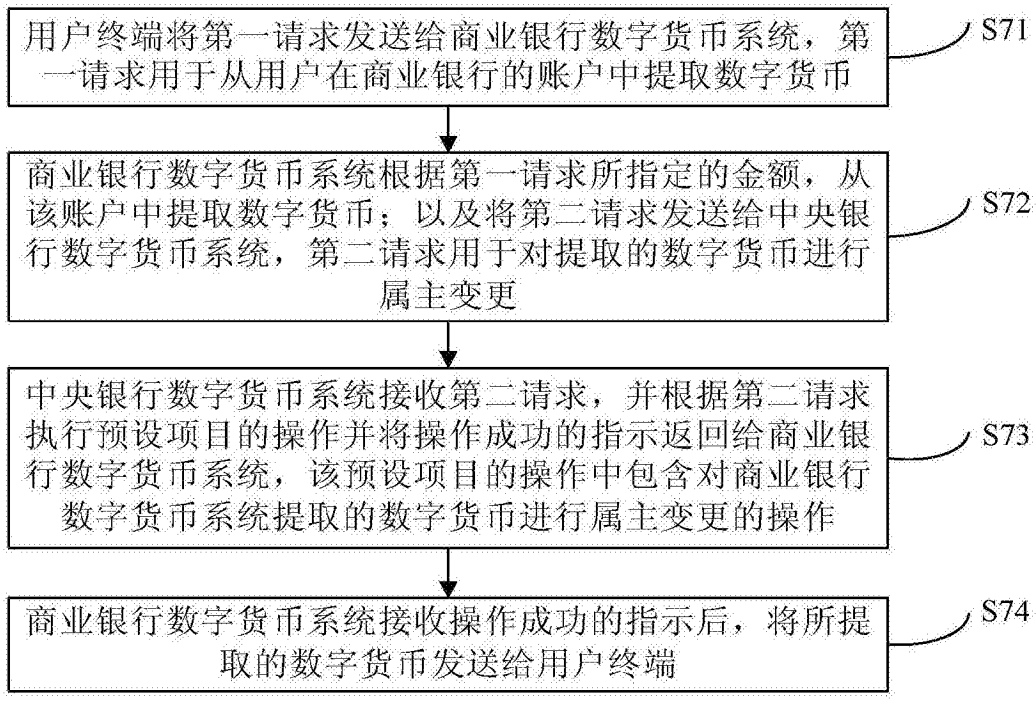

用户终端将第一请求发送给商业银行数字货币系统，第一请求用于从用户在商业银行的账户中提取数字货币
S71
商业银行数字货币系统根据第一请求所指定的金额，从该账户中提取数字货币；以及将第二请求发送给中央银行数字货币系统，第二请求用于对提取的数字货币进行属主变更
S72
中央银行数字货币系统接收第二请求，并根据第二请求执行预设项目的操作并将操作成功的指示返回给商业银行数字货币系统，该预设项目的操作中包含对商业银行数字货币系统提取的数字货币进行属主变更的操作
S73
商业银行数字货币系统接收操作成功的指示后，将所提取的数字货币发送给用户终端
S74

图7

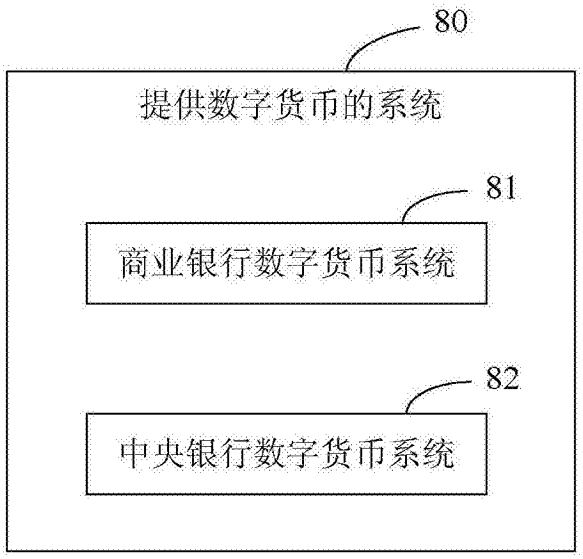

80
提供数字货币的系统
81
商业银行数字货币系统
82
中央银行数字货币系统

图8