2017年·第11期
栏目编辑：梁丽雯 E-mail:liven_01@163.com

# 央行数字货币模型探析*

■ 中国人民银行衡阳市中心支行 李卓伦

**摘 要:** 根据中国人民银行公开信息，基于区块链的数字票据交易平台已测试成功，数字货币应用进入试点阶段。本文以比特币及区块链为切入点，提出一种基于区块链技术的央行数字货币模型，从客户端、传输端和终端3个方面分析了模型的安全性，为数字货币研究提供了一种思路。

**关键词:** 央行数字货币；区块链；安全研究；模型架构

数字货币的出现被视为是货币形态的又一次重大革命，因此其发展备受学术界、业界和各国央行关注。根据中国人民银行公开信息，基于区块链的数字票据交易平台已测试成功，这意味着数字货币的试点应用场景已建立。目前已经有欧洲央行、德国央行、加拿大央行、英国央行等正在认真考虑使用数字货币。研究表明，数字货币可能是一个对于所有人来说都成本更低的选择。

## 一.参考模型

（一）比特币

比特币是基于分布式账本的一种加密数字货币，是构建在一种新型的密码技术之上且具有潜力彻底改革金融体系的新协议。比特币中构建了对等货币和一个支付系统，而不依赖任何的第三方，其展现了货币的一种新概念，因为它是一种不是由任何一家央行发行但却被人们接受的“货币”（广义货币，在部分国家和商户认可且可用于交换商品及服务），从而挑战了全球数字支付系统和对等电子金融机构。协议被设计成从集中式货币体系转向个人分布式网络，比特币提供所有交易公开的公共分类账本存储并且可以被连接到比特币网络的任何节点访问。比特币数据包括用户提出的汇款交易、计算涉及交易验证和更新的数据结构。

（二）区块链技术

比特币中的分布式记账称为区块链。区块链是比特币协议的关键创新，它可以被视为包含所有账号和余额的分布式数据结构，其能够在网络中建立点对点之间可靠的信任，使得价值传递过程去除了中介的干扰，既公开信息又保护隐私，既共同决策又保护个

**作者简介：** 李卓伦(1983-)，男，湖南祁东人，工程师。
**收稿日期：** 2017-08-25
*本文仅代表作者个人观点，不代表作者所在单位意见。

体权益，这种机制提高了价值交互的效率并降低了成本。除点对点传输技术外，区块链还综合了分布式存储、共识信任机制和加密算法等。

在传统货币的交易模式中，银行管理账户采用的是中心化管理。由银行建立中心数据库，每个人的银行账户信息和以及账户里有多少余额都由银行进行集中管理。而基于区块链技术的交易模式则剔除了银行作为中心数据库的角色，如每个比特币用户的电脑都是一个节点，每个节点都能存储数据，节点和节点相连形成了巨大的网络。区块链的信任机制取决于账本的透明和可共同维护等特性，交易（匿名）通过其他用户验证并达成共识后写入区块，区块信息可以被任何人查询、验证但不可更改。区块信息向使用区块技术的整个网络广播，每个用户节点都保存一份区块副本，即区块信息的函数映射，从而达到验证的目的。由于所有用户都拥有区块副本，非法修改过的区块将无法通过验证，这一安全机制极大地提高了区块链的信息安全性和完整性。当不同的区块在网络上形成链接时就成为了区块链。

区块链在未来还可能实现价值的转移，例如债券、股票等有价金融证券，以及房产、汽车等产权都可以利用区块链登记、交易。同样，区块链还可以应用于电子票据、支付清算、供应链金融等方面，见表1所列。

表1 区块链技术应用

| | | |
|---|---|---|
| 区块链1.0 | 货币 | 数字货币：比特币、其他类似比特币、央行法定数字货币 |
| 区块链2.0 | 可编程金融 | 智能合约：证券交易、产权登记、防伪、 |
| 区块链3.0 | 其他行业 | 身份认证、公证、物流、审计、投票等 |

## 二.对比参考

比特币是数字货币的典型应用，但比特币和央行数字货币有着显著区别。

根据公开资料显示，央行数字货币架构有以下特点：一是央行数字货币是国家法定货币，其本质是人民币的另一种存在形式（类似于比特币的一种电子货币形式）；二是数字货币在使用和流通过程中的安全性需要应用密码技术来保障；三是在产生、流通、清点核对及消亡全过程登记，可参考区块链技术，建立集中、分布相对均衡的簿记登记中心；四用户身份认证采用“前台自愿、后台实名”的原则，既保证用户隐私，又规避非法交易的风险；五是央行数字货币有中心且基于现行“中央银行—商业银行”的二元体系来完成，见表2所列。

表2 央行数字货币与比特币对比

| | 技术 | 去中心化 | 法定货币 | 匿名交易 |
|---|---|---|---|---|
| 央行数字货币 | 区块链 | 否 | 是 | 是（但可追踪） |
| 比特币 | 区块链 | 是 | 否 | 是（不可追踪） |

## 三、数字货币在央行的应用构想

作为法定数字货币必须由国家主权保障，由央行或者央行授权发行。发行过程中，须支持手机移动支付网络交易、虚拟网络与现实交互、现实与现实交互等多种场景使用。要能打通线上与线下，既有自己独立的运行体系，又能实现与现代支付系统的无缝衔接。

央行数字货币通过密码算法为基础来实现。在纯数字货币技术上，利用芯片技术、用安全芯片来保护秘钥和算法，是现阶段网络环境下的较为稳妥的选择。

（一）基于国密算法的客户端应用构想

首先是利用国密算法SM2生成一对秘钥，即用户的公钥和私钥。该秘钥用于数据加密，用公钥加密时仅私钥可以解密。所有用户公钥对外发布、公开可见，同时保持私钥机密性。当用户A需要同用户B发生交易时，采用B的公钥对数据进行加密。当加密完成后仅B用户可以使用自己的私钥对数据进行解密。

其次是用户认证，采用国密算法进行数字签名，其过程是加密的逆向操作。例如用国密算法SM3将经

过处理的用户信息的信息摘要值发送给对方，用户A真实姓名为张三，当张三与用户B李四交易时，先由张三通过信息摘要算法SM3输出一段固定值“a3b52b4f”这段数值是用户A的代码，仅输入“张三”才可以得到，如果输入李四或其他人名都会得不同的结果。这时候A用户使用私钥加密，仅用户A公钥可以解密，而公钥是对外公开的，因此所有人都可以拥有用户A的公钥从而验证是用户A发起的交易。由于可解密的公钥对应的是用户A的私钥（仅用户A有），因此用户A对其私钥数字签名的信息不可抵赖，其他用户也可以相信是由用户A发起的交易。根据用户身份认证采用“前台自愿、后台实名”的原则，在后台还是可以追溯到“a3b52b4f”代表的是用户张三，而前台用户只是看到代表张三身份的一串唯一的代码“a3b52b4f”。

（二）基于量子通信技术的传输端模型构想

随着科技的发展，量子密码和量子通信在未来将一步一步走向实际应用，因此，在实际传输过程中可以考虑通过量子密码来将传统数字信号转换为光信号。量子密码术与传统的密码系统不同，它依赖于物理学作为安全模式的关键，而不是数学。实质上，量子密码术是基于单个光子的应用和它们固有的量子属性开发的不可破解的密码系统，因为在不干扰系统的情况下无法测定该系统的量子状态。

现代通信密码学的主要研究方向是将隐秘的信息在公共的不安全环境（如互联网）中传输。这时就需要利用加密解密原理。纯粹的量子通信是针对整个通信的物理安全信道的，其优势是近乎完美的机密性，但对于海量数据的加密实用性并不高，因此，采用量子通信与传统密码学相结合不失为一种解决方案。即将秘钥通过量子通信环境传输，但通过秘钥加密的密文通过公共信道传输。

（三）基于云架构和5G通信的终端模型构想

云计算和5G技术的发展为未来央行数字货币提出一种全新的模型构想。海量区块数据与现有网络传输带宽的矛盾十分突出，5G正是完美的解决方案。与目前4G技术相比，5G其峰值速率将增长数十倍，从4G的100 Mbit/s提高到几十Gbit/s。也就是说，1秒钟可以下载10余部高清电影，可以更好地满足物联网海量数据接入场景。此外端到端延时将从4G的十几毫秒减少到5G的几毫秒。同时5G技术将实现“万物互联”，将现有互联网扩充到物联网，并实时保存用户在线状态，从而从本源上解决离线交易这一问题（这也是央行电子现金推广中的一个痛点）。

云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问，进入可配置的计算资源共享池（资源包括网络、服务器、存储、应用软件、服务），资源能够被快速提供，只须投入很少的管理工作，或与服务供应商进行很少的交互。可由央行牵头，各大商业银行组成私有云，同时利用大型机构在我国各省（及重要城市）组建二级云节点，从而形成一个“私有联盟云”。采用IaaS（Infrastructure as a Service）基础设施即服务模式，由各大云节点完成所有央行数字货币体系的基础建设、运行、维护等工作，对外提供服务。而用户端仅需要使用基于移动设备（手机或电脑）的客户端软件即可，从而大大减少了用户的支出，从而减轻了用户端推广的压力。同时私有云对信息的安全提供了更高的保障。

## 四、央行数字货币面临的挑战

首先是对现有区块链技术的改良，目前区块链仅支持每笔交易为7秒，而在现实交易中，以“双11”为例，交易峰值为每秒10万笔以上，在央行应用层面考虑业务峰值至少要达到“双11”峰值。因此，是否最终采取区块链技术或者对现有区块链技术进行改良，将是央行数字货币面临的首要问题。其次，是M0与M1之间的货币转换。当终端用户使用央行数字货币时，与银行账户之间的存款转换（存、取交易）牵涉到系统架

（下转P33）

预测金融风险，加强对相关数据的收集，及时发现违规操作和潜在的交易问题，提高安全级别，避免问题的发生。除此之外，金融机构还可以采取应用对接、系统嵌入等方式，将规章制度、监管政策和合规要求翻译成数字协议，避免人工干预，通过标准化的管理方式避免出现歧义，保证工作质量。

（二）对相应的管理体制进行创新

在当前的金融科技体系当中，政府是非常重要的参与者，起到重要的作用，然而其工作内容复杂，自身存在一定的矛盾性，不仅要对市场进行服务，还要对市场进行管理和引导。因此，为了保证工作效率最大化，必须拿捏好管理和调控的尺度，避免矫枉过正。由于我国国情的特殊性，再加上政策和体制存在一些问题，导致和科学技术发展相比，与之对应的政策制度都比较落后。体系、制度没有与时俱进，导致其不能发挥最大作用，不能最大程度地促进金融科技的发展。因此，在以后的发展中，政府要有效发挥自身的服务职能，对相关法律法规进行制定，借鉴发达国家的处理办法，对不合理的法律法规进行修改，同时结合工作中发现的问题，有效进行处理和弥补，提高工作的实效性。当法律法规可以有效发挥作用，就可以保证市场的稳定，为金融科技的发展创造良好的条件。FTT

参考文献：

[1]王宇超．互联网金融监管的必要性与核心原则[J]．科技创新导报，2016(22):113-114.

[2]刘绪光，杨帅．我国互联网金融监管可借鉴沙箱创新[J]．金融经济:市场版，2017(3):36-37.

[3]陈天华．依靠科技创新，提高金融监管和金融服务水平——访中国人民银行天津分行何成玉副行长[J]．金融电子化，2011(6):11-17.

[4]蔡元庆，黄海燕．监管沙盒:兼容金融科技与金融监管的长效机制[J]．科技与法律，2017(1):68.

[5]叶文辉．英国“监管沙箱”的运作机制及对我国互联网金融监管的启示[J]．华北金融，2016(12):37-40.

（上接P30）

构，在初始的设计应考虑如何实现与现有货币发行系统和发行基金（现金实物）之间的动态平衡。第三，央行数字货币对现有银行体系的冲击是无法避免的。如果采取用户与央行直接开立账户并进行交易的方式，将给现有“央行-商业银行”的二元体系带来巨大冲击。如维持现有二元体系，则对现有商业银行的业务架构和业务支持系统也将带来巨大挑战。第四，当前比特币等数字货币的广泛应用对央行数字货币推向市场的时限提出了重大挑战，如太晚推出或将面临市场已被完全占领的情况，具体可参照目前移动支付市场现状，即支付宝、微信支付占据绝大多数市场的情况下，银行卡支付市场萎缩，如不使用行政手段，容易面临被市场淘汰的趋势。FTT

参考文献：

[1]中国人民银行数字货币研究项目组．法定数字货币的中国之路[M]．中国金融，2016(17):45-46.

[2]范一飞．中国法定数字货币的理论依据和架构选择[J]．中国金融，2016(17):10-12.

[3]姚前．中国法定数字货币原型构想[J]．中国金融，2016(17):13-15.