



# 理解央行数字货币: 一个系统性框架

姚前

中国人民银行数字货币研究所\*, 北京 100088

E-mail: yaoqian@pbc.gov.cn

\* 作者系中国人民银行数字货币研究所所长, 本文仅代表个人学术观点, 不代表所在机构意见.

收稿日期: 2017-11-02; 接受日期: 2017-11-09; 网络出版日期: 2017-11-15

**摘要** 当前, 法定数字货币的研发正引起政策制定者、监管机构、产业界、学术界的广泛兴趣, 但对于它的具体形态, 尚未有清晰的概念和蓝图. 本文建立了一个系统性框架, 从价值内涵、技术方式、实现手段、应用场景等 4 个全新的维度, 剖析了法定数字货币的本质和内涵. 研究认为, 法定数字货币在价值上是信用货币, 在技术上是加密货币, 在实现上是算法货币, 在应用场景上则是智能货币. 与现有的私人数字货币和电子货币相比, 法定数字货币将呈现出全新、更好的品质. 让货币价值更稳定, 让数据更安全, 让监管更强大, 让个人的支付行为更灵动, 让货币应用更智能, 不仅能很好地服务大众, 同时又能为经济调控提供有效手段, 还能为监管科技的发展创造坚实的基础, 这些优秀品质是中国法定数字货币所追求的目标.

**关键词** 法定数字货币, 信用货币, 加密货币, 算法货币, 智能货币

## 1 引言

近几年来, 数字货币发展迅速, 正成为大家热议的焦点, 其中关于法定数字货币 (digital fiat currency, DFC) 的研发, 更是引起政策制定者、监管机构、产业界、学术界的广泛兴趣. 目前, 各国中央银行更多关注的是如何将分布式账本技术 (distributed ledger technology, DLT) 应用于资金批发市场的实时全额支付 (real-time gross settlement, RTGS), 而对于法定数字货币的具体形态, 尚未有清晰的概念和蓝图.

早在 2015 年, 国际清算银行下属的支付和市场基础设施委员会<sup>[1]</sup> (Committee on Payments and Market Infrastructures, CPMI) 将法定数字货币定义为加密货币 (crypto-currency). 随后, Zhou<sup>[2]</sup> 提出数字货币可分为基于账户和不基于账户两种. 继 Broadbent<sup>[3]</sup> 提出央行数字货币 (central bank digital currency, CBDC) 的概念后, Fan<sup>[4]</sup> 指出央行数字货币主要属于现金 (M0) 范畴. Yao 则提出了基于账户 (account-based) 和基于钱包 (wallet-based) 的数字货币概念<sup>[5]</sup>, 并设计了一个基于银行账户和数字货币钱包分层并用的架构<sup>[6]</sup>, 以使法定数字货币可以有机融入“中央银行-商业银行”二元体系, 复

**引用格式:** 姚前. 理解央行数字货币: 一个系统性框架. 中国科学: 信息科学, 2017, 47: 1592-1600, doi: 10.1360/N112017-00218

Yao Q. Understanding central bank digital currency: a systemic framework (in Chinese). Sci Sin Inform, 2017, 47: 1592-1600, doi: 10.1360/N112017-00218

用现有的成熟的金融基础设施,避免狭义银行化影响.与之相似,Koning<sup>[7]</sup>根据是否基于央行账户,将法定数字货币区分为央行数字账户(central bank digital account, CBDA)和央行数字货币(CBDC).Bordo和Levin<sup>[8]</sup>将法定数字货币区分为CBDC账户和CBDC代币.而Bech和Garratt<sup>[9]</sup>则提出央行加密货币(central bank cryptocurrencies, CBCCs)的概念,并从发行者(央行或其他)、货币形态(电子或实物)、流通范围(全局或局部)、流通机制(中心化或去中心化)4个角度对CBCC的特性进行了阐述.

上述各种提法既相似也有一些微妙的不同,法定数字货币前所未有,畅想它的未来形态,需要有更丰富的想象力和更广阔的视野.不同于已有研究,本文建立了一个系统性框架,从价值内涵、技术方式、实现手段、应用场景等4个全新的维度,剖析了法定数字货币的本质和内涵.本文研究认为,法定数字货币在价值维度上是信用货币,从技术上看应该是加密货币,从实现方式来看则是算法货币,从应用场景来看是智能货币.理想中的法定数字货币应具备全新的品质,从而超越现有的私人数字货币和电子货币.

## 2 在价值维度上法定数字货币是信用货币

法定数字货币是由中央银行发行,采用特定数字密码技术实现的货币形态.与实物法币相比,数字法币变的是技术形态,不变的是价值内涵.本质上,它仍是中央银行对公众发行的债务,以国家信用为价值支撑.这使其天生就具有两个私人数字货币无法比拟的优势.

(1) 法定数字货币有价值锚定,能够有效发挥货币功能.相比交易媒介功能,货币作为计价手段的功能是第一位的,而作为计价功能,货币价值的稳定性至关重要.对于货币的价值储藏功能更是如此.货币需要有价值锚定,才能有效发挥货币功能.

回顾历史,各种货币形态均有价值锚定.商品货币、金属货币的价值锚定来源于物品本身的内在价值.金本位制度下,各国法定货币以黄金为价值锚定.Bretton森林体系崩溃以后,各国法定货币虽不再与黄金挂钩,但是以主权信用为价值担保.到了法定数字货币时代,这一最高价值信任将继续得到保留和传承.

反观以比特币为代表的去中心化类私人数字货币,其价值来源在哪里?是自由主义者对货币发行非国家化的Utopia情怀,还是挖矿消耗的计算资源?是市场对未来区块链技术发展的乐观预期,还是短期投机暴利下的非理性诱惑?从目前来看,应该是投机因素居多.从公共经济学视角看,比特币等私人类数字货币不具备提供“清偿服务”和“核算单位价值稳定化服务”等公共产品服务的能力,在交易费用上亦不具有明显优势,这些缺陷决定了其难以成为真正的货币<sup>[10]</sup>.

(2) 法定数字货币有信用创造功能,从而对经济有实质作用.在非信用货币时代,人们眼中的货币是无意义的.李嘉图、Anton Menger、Walras等古典经济学家们倾向于认为,商品货币、金属货币等非信用货币对经济是中性的,它们只是覆盖在实体经济的面纱,对经济无实质作用,仅会引起价格的变化.

而在信用货币时代,货币本身就是信用,实质上是发行主体信用的证券化,具有金融属性,货币创造过程即是一种信用创造过程.Keynes主义者、货币主义学派、理性预期学派以及金融加速器理论从不同角度分别论证了各种情况下货币非中性的微观机理和宏观表现,支持了货币在经济中的关键作用.

事实也表明,货币的信用创造功能对于现代经济至关重要,尤其是金融危机时刻的流动性救助,对于防止危机传染、助推经济快速复苏有着重要的意义.典型的例子是2008年国际金融危机爆发后,

美联储主动创设多种流动性支持工具，将援助对象由传统的商业银行，扩展到非银行金融机构、金融市场和企业，迅速阻止了危机的进一步传染和恶化，这正是当前美国经济能够在全球率先复苏的关键因素。

从完全放任自由的市场到中心化机构的出现，是市场自然而然演化的结果。具有讽刺意味的是，以自由市场为圭臬的市场原教旨主义者，竟然不相信自由市场的选择。诸如比特币等，按照算法设计，每4年产生的数量减半，最高上限为2100万个，其实是货币的“返祖”，相当于重新披上了商品货币和金属货币的面纱，对经济没有实质意义，仅起到克服物物交换困难的便利交易作用。在日益复杂的信用经济时代，若以比特币为货币，无疑是一场灾难。

除了上述两个优势，与传统法币相比，法定数字货币还有一个优势是，有助于改进法币的价值稳定。

以国家信用为价值支撑的法币，在不同人眼里有着不同评判，有人认为其具有最高价值信任，也有人认为它只是利益再分配的工具。比如自由主义者认为，国家有着财政赤字货币化的冲动，由其垄断货币发行权，容易导致通货膨胀，因此他们宣扬自由市场的力量，建议废除国家货币发行垄断权，实行货币自由发行和竞争，以维持价格稳定。此外，中央银行制定货币政策规则时，通常会设定2%的目标通胀水平，也经常被解读为通胀倾向。

对于前者，可以通过提高央行独立性来解决。目前，在政府治理机制比较完善的国家中，财政赤字货币化行为已得到很好的抑制。而对于后者，则可通过引入法定数字货币，来降低货币政策规则上设定2%目标通胀水平的必要性。数字货币环境下，有效负利率政策将成为可能，中央银行可能不再需要设定目标通货膨胀率缓冲，理论上中央银行的目标通货膨胀率可降至0。从这角度看，法定数字货币或有助于改进法定货币的价值稳定。

### 3 在技术维度上法定数字货币是加密货币

法定数字货币是数字经济发展的基石。未来的数字经济一定是加密数字经济，而不是明文数字经济。就此而言，法定数字货币的技术本质，理应是加密货币。加密技术是法定数字货币实现技术安全和可信的关键要素。

具体而言，在法定数字货币本身的设计上，需要运用密码学理论知识设计法定数字货币特定的表达形式，保障数字货币的可流通性、可存储性、不可伪造性、不可重复交易性与不可抵赖性等；在法定数字货币交易过程中，需要运用加密技术、分布式账本技术、可信云计算技术和安全芯片技术来保证端到端的安全，防止被窃取、篡改、冒充<sup>[11]</sup>；在法定数字货币的用户体验上，需要结合隐私保护技术与分布式账本技术，在为用户提供不同于传统电子支付的点对点支付体验的同时，通过隐私保护技术确保用户数据的安全，避免敏感信息的泄露，且不损害可用性；在法定数字货币监管方面，利用数字货币“前台自愿，后台实名”的特性，通过安全与隐私保护技术来管理相关数据使用权限，确保大数据分析等监管科技有用武之地<sup>[12]</sup>。

近几十年来，加密货币理论创新与实践进展迅速。在理论上日渐成熟。Chaum<sup>[13]</sup>最早提出一种具有匿名性、不可追踪性的电子现金系统。Dai<sup>[14]</sup>提出了一种名为b-money的匿名的分布式电子现金系统。Jakobsson和Juels<sup>[15]</sup>提出工作量证明机制。Szabo<sup>[16]</sup>发明了Bitgold。Nakamoto<sup>[17]</sup>发表经典论文《比特币：点对点的电子现金系统》，提出了一种去中心化的完全通过点对点技术实现的电子现金系统。实际上比特币的区块链技术融合了当时各种加密技术的最新进展。

加密货币理论在实践上成果丰富。自比特币问世以来，各种替代加密货币层出不穷。截至2016年，

共有 600 多种数字货币. 这些加密货币进一步利用各种数字货币技术, 对比特币进行了扩展与变形, 很多试验进展具有较强的学术创新性.

加密货币理论研究和实验成果为法定数字货币提供了丰富、有益的参考. 目前, 一些国家的央行也都基于分布式账本技术进行央行数字货币试验, 如加拿大央行的 Jasper 项目<sup>[18]</sup>、新加坡金管局的 Ubin 项目<sup>[19]</sup>、香港金管局的 Lionrock 项目<sup>[20]</sup>. 欧洲中央银行和日本央行联合开展的 Stella 项目<sup>[21]</sup>则对分布式账本技术是否能够取代实时全额结算系统 (RTGS) 进行研究. 现在看, DLT 取代 RTGS 还为时尚早, 应将数字货币和区块链“松绑”<sup>[22]</sup>. 法定数字货币对区块链技术的借鉴, 应根据实际业务需求在改造的基础上灵活应用. 就此而言, Danezis 和 Meiklejohn<sup>[23]</sup>提出的 RSCoin 系统的设计理念值得参考, 该系统站在中央银行视角, 不拘泥于区块链技术, 力图实现一种受中央银行控制的、可扩展的加密数字货币<sup>[24]</sup>.

Koning<sup>[7]</sup>把账户 (account) 和 (代) 币 (currency 或 token) 这两个最重要的概念拎了出来, 非常有趣. 从演化路径看, 央行发行法定数字货币其实是从账户 (account) 向央行代币 (token) 延伸的过程; 而加密货币从最开始的公有链到后续的联盟链、私有链, 则可看作是从代币 (token) 往账户 (account) 方向的推进. 在这里账户、代币、币之间其实是你中有我、我中有你的关系. 所以, 央行发行法定数字货币, 采用 CBDA, CBDC, CBCC 混合的思路或更为稳妥.

说到 token, 很自然就会想起 tokenization 技术, 比如支付标记化 (payment tokenization) 技术. 这是由国际标准化组织 EMVCo 于 2014 年正式发布的一项支付技术. 支付标记化技术采用标识符号替代了传统银行卡卡号和有效期, 从根本上杜绝敏感信息泄露的可能, 降低了欺诈交易的发生概率, 并可以通过域控功能限定交易场景 (如交易类型、使用次数、交易金额、有效期、支付渠道、商户名称等), 使支付更加安全. 探索中国法定数字货币的表达方法, 进一步研究数字货币基础数学模型, 包括属性、发行者、所有者、使用权限、使用范围、数字签名、加密、防伪等, 并建立其识别和描述模型, 无疑是必要的<sup>[12]</sup>. 支付标记化技术对便利性、隐私性和安全性的平衡处理, 以及采用的域控设计理念, 值得法定数字货币借鉴.

随着可信云计算、安全芯片与隐私保护等加密技术的成熟, 法定数字货币将以用户为中心来管理, 这将大大减少货币运营中的诸多中间环节, 央行也可以直接穿透到最终用户, 为经济调控提供一种全新的手段.

#### 4 在实现维度上法定数字货币是算法货币

在实际的货币业务中, 法定数字货币是算法货币, 包含 3 层意思. 一是在法定数字货币的设计上, 可以采用各种加密算法来保障安全可信的同时, 如 Hash 算法、Fitzner 加密算法、盲签名、环签名等, 为将来的新兴算法也预留了一些特殊字段. 二是在货币发行环节, 法定数字货币设计上有可执行脚本的考虑, 将来可以使用预设可靠的算法规则来进行发行. 说起发行算法, 很自然就会想起比特币的 POW 共识机制, 比特币煞有介事地通过挖矿的算法机制来进行发行, 但这种规则与交易手续费捆绑在一起, 机械僵化, 根本上脱离了社会经济实际, 无法适应现代宏观经济调节的需求. 法定数字货币发行的算法规则, 理应是一套能在保持币值稳定的前提下, 让货币供给充分适应宏观经济多变量环境变化的智能规则. 以目前的技术水平看, 有可能是一套精致的、基于机器学习算法的人工智能 (AI) 模型. 三是可以运用大数据, 对货币的发行、流通、储藏等进行深度分析, 了解货币运营规律, 为货币政策宏观审慎监管和金融稳定分析等干预需求提供数据支撑.

一直以来, 货币经济学家们对货币政策规则展开广泛而深入的研究, 试图为中央银行的货币供给

提供理论指导，Taylor 规则、Friedman 的单一规则、芝加哥学派的货币主义等货币学说，在方法论上从定性扩展到定量研究，建立了计量经济学和实验经济学，以期为中心银行理解和把握现实经济世界提供精准的工具。某种意义上来说，经济学家们为中心银行构建的货币发行决策模型，其实是初级的 AI 模型。

遗憾的是，由于数据搜集、存储和计算能力受限，这些 AI 模型尚未能在大规模的机器学习中得到优化和改进，仅是中央银行货币决策的辅助工具。比如，模型学习的数据维度小，频度低，时滞长，导致模型学习的知识量不足，过度参数化，预测误差大；模型计算能力有限，无法遍历各种决策空间，决策逻辑相对单一，难以实现决策全局最优。这就决定了目前的央行货币发行更多依靠专家决策，专家的学识、智慧和经验当然值得推崇，但人脑决策难免存在误差，甚至有可能失误，这正是现代货币政策备受诟病的原因之一。

目前货币运行相关数据基本通过后验式统计与估算来形成。这样就使得货币在现实流通中存在较大不确定性，即当货币发行以后缺乏实时有效的监控手段，在流通中实际发挥交易手段、流通手段的货币到底有多少？这些货币被应用的主要场景有哪些？货币流通速度怎么样等问题，都很难找到确切的答案。以至于有的国家央行官员不无调侃地说，我们真不知道目前实际发挥流通手段、交易手段的纸币规模到底有多少，这是一个黑盒子。

但数字货币的出现改变了这一局面。尤其是对法定数字货币而言，其货币的创造、记账等都是由央行或者央行组建的联盟中心来完成的，央行是造币者、发行者，一些关键核心节点是记账者，普通节点是运用数字货币进行交易的经济主体，在这一技术体系中，央行拥有最高的决策和业务权限。因此，在这一角色定位下，在数据适当脱敏的情况下，大数据分析就有了用武之地。

法定数字货币从系统设计之初，就需要在法律许可的范围内，重点考虑大数据顶层设计及相关的基础设施建设。从系统设计上，要注重大数据基础设施的鲁棒性和拓展性，根据数据层、接口层、服务层和应用层划分，保证数据收集、分析模型、应用接口都具有良好的安全性、灵活性和一定程度的开放性。从时域上，要提取数字货币发行、流通、交换、贮藏、回收的全生命周期关键基础数据，为进一步的模型构建、仿真、分析和调控夯实基础。从空间域上，构建数字货币运行分布云图，清晰勾画法定数字货币运行的规模、地点、时间，并进行空间标注，形成数字货币运行分布的实时云图，清晰地了解数字货币的运行区域和投放重点域，为精准施策做好支持。

基于以上基础，中央银行科学遴选相关数字货币分析指标体系，从可观性、可控性、相关性和稳定性维度，测度关键的数字货币总量型指标和价格信号类指标，进一步仿真分析数字货币调控工具类指标的影响，从而为货币政策制定与实施提供有益的决策参考<sup>[25]</sup>。

当前技术以 Moore 定律在不断的发展。随着自动搜索、网络爬虫、自动分类等数据搜集技术的持续发展，传感器、信息识别、生物识别等数据捕捉工具的不断丰富，现代高性能计算集群的计算性能和存储功能的快速提高以及通信技术的更新换代，基于大数据分析，将机器学习算法和人工智能技术应用于货币政策，探索开发完备先进的货币发行 AI 模型，是否可以先行先试？我们认为这是可能的，我们已对法定数字货币发行的 AI 模型和学习算法展开了研究，探索性地提出具体框架，包括模型设计和学习算法，并基于通过外汇市场开展货币投放的简单场景，进行了初步的试验。结果表明，虽然存在一定的识别误差，但模型的整体效果还不坏。

总之，预计未来，在法定数字货币环境下，通过预设、可靠的程序算法规则，在保证币值稳定的前提下，由经济系统自发、内生地决策货币供应量，自动地发行和回收货币，将成为可能。中央银行的角色或许将不仅仅是货币发行量的决策者，还是货币发行算法规则的设计者。

## 5 在应用维度上法定数字货币是智能货币

法定数字货币不仅是简单地将货币进行数字化和网络化,更重要的是可以让货币变得更加智能化.与信用卡、银行储蓄卡、支付宝、微信支付等传统电子支付工具相比,法定数字货币将会呈现出全新、更好的品质.

(1) 法定货币的用户体验将变得更加智能.当前,智能科技技术正在快速地融入人们的生活.移动芯片中包含人工智能单元正成为主流,硬件终端的智能化将与各个软件系统的智能化形成交互,从而创造出全新的智能化世界.在这智能化的世界里,需要有智能化的货币.智能合约执行自动且可信,可以在技术上提供降低合同违约和信用违约风险的新手段,是法定数字货币发展的一个方向.

Yao<sup>[26]</sup>研究了数字货币在跨行调款场景中的应用,发现通过数字货币的条件支付功能,能够很好地解决交易双方的信任问题,以及交易过程中资金流与交易流的同步问题.Xu和Yao<sup>[27]</sup>研究了基于区块链技术的数字票据交易平台方案,并结合数字货币的清算结算功能,设计了一个由智能合约管理的流动性节约机制(LSM),结果表明央行数字货币的引入大幅简化了票据交易流程.

此外,去中介化的点对点支付,也将带来很多全新的用户体验,它能给数字货币插上翅膀,让用户支付的能动性大大提高,并在货币的支付功能上延伸出更多智能化的功能,从而创造各种智能化的商业应用.

从现状看,很多国家研究更多是超级央行、CBDA的思路,类似于构建一个央行层面的超级支付宝.而在中国,由于支付宝、微信支付等私人支付工具非常发达,“无现金社会”、“无现金城市”等词语频频出现,最近讨论的货币市场基金是否推高融资成本的问题,其实质意义还在滥觞.私人支付工具的发达及其日益垄断的局面,一定会倒逼监管机构有所行动;商业银行也必须严肃思考狭义银行以及退为资金批发商和系统后台的可能性.按常理,零售端的支付工具本该由央行数字货币为主来实现,但私人部门已经捷足先登,一方面私人部门的创新能力值得称道,另一方面央行必须奋起直追.无论如何,在数字资产的世界里,央行数字货币不能缺位.中央银行发行零售端数字货币,对于健全社会支付体系、维护金融稳定以及加强央行的货币地位,具有重大而深远的意义.

应该说,用户已经体验到了私人支付工具的便利性,对法定数字货币的用户体验心存疑虑.实际上相比传统货币,无论是实物货币,还是电子支付工具,法定数字货币对持币者的好处是可以专门探讨的.传统纸币,有发行机构的信息,但不会有持有人登记的概念,更不会保存流转过程中全生命周期的信息,而且这些信息的主导权,还在持币者的手中.这样一种根本性的差异,使得法定数字货币的持币者,对于自己资金的自主可控,有了一个质的飞跃.

(2) 货币政策执行变得更加智能.目前,学者们已经敏锐地感知到,货币形式的数字化对于提高货币政策有效性能发挥积极作用.如Stiglitz<sup>[28]</sup>研究了电子货币系统的宏观经济管理.我们对这个思路进行详细论证时发现,法定数字货币的可追踪性和可编程性将会让货币政策执行变得更加智能,更加有效.进而,我们尝试着提出了一个称之为“前瞻条件触发(forward contingent)”的货币生效设计.通过这一设计,目前困扰中央银行的传导机制不畅、逆周期调控困难、货币“脱实向虚”、政策沟通不足等货币政策困境,有可能得到很好的解决.

比如通过“时点条件触发(time contingent)”货币生效设计,让货币只有在商业银行放贷时才能生效,从而减少货币政策传导时滞,并避免货币空转;通过“流向主体条件触发(sector contingent)”货币生效设计,限定商业银行贷款流向部门和主体,精准定向货币投放,实施结构性货币政策,减少货币空转,提高金融服务实体经济能力;通过“信贷利率条件触发(loan rate contingent)”货币生效设计,让商业银行信贷利率满足关于基准利率的函数,从而实现基准利率向贷款利率的有效实时传导;通过“经

济状态条件触发 (economic state contingent)”设计, 根据宏观经济状态, 逆周期调整商业银行对中央银行的资金归还利率, 从而减少商业银行风险特征及其贷款行为的顺周期性, 实现经济的逆周期调控。

同时, 由于法定数字货币在发行时即内置了这些条件设定, 并能被商业银行公开获知, 而这些条件设定恰是央行货币政策逻辑和意图的反映, 因此法定数字货币兼具了前瞻指引 (forward guidance) 功能。

## 6 结论

对于货币持有者而言, 他们最关切的货币品质不外乎有两点: 一个是不能“假”了, 另一个是不能“毛”了。前者是对铸币技术的要求, 后者是对货币背后的价值支撑的要求。这种关切对数字货币来说也是概莫能外。前文所阐述的法定数字货币 4 个维度, 即在价值上是信用货币, 技术上是加密货币, 实现上是算法货币, 应用场景上是智能货币, 完全可以落到这两个根本点上来, 只不过数字货币技术的应用, 使得法定数字货币还会有更多的安全便捷智能等方面的特性要求。

考虑到中国的支付环境非常发达, 中国的法定数字货币, 必须在品质上超越现有的各种私人支付工具。让货币价值更稳定, 让数据更安全, 让监管更强大, 让个人的支付行为更灵动, 让货币应用更智能, 不仅能很好地服务大众, 同时又能经济调控提供有效手段, 还能为监管科技的发展创造坚实的基础, 这应是中国法定数字货币追求的目标。

中国有句古语, “取法乎上, 仅得其中; 取法乎中, 仅得其下”。本文建立了一个系统性框架, 剖析了法定数字货币的 4 个维度, 目的就是为了取法乎上, 树立一个远大的理想和目标。但我们也清醒地认识到, 这个远大目标的实现不可能一蹴而就, 需要根据现实情况分步实施。

目前, 各国探索的法定数字货币, 主要还是为了提高支付效率, 而中国在电子支付方面已经非常发达。在当下, 我们的弊端似乎不是效率有问题, 而是需要兼顾效率和安全, 既提倡创新也注重风险防范, 在弥补零售端数字法币缺失的同时做好私人支付工具的监管, 然后再逐步探索法定数字货币品质的进一步提升, 应该都是比较稳妥的路径选择。这也契合当前技术发展的进程, 比如数字货币的可编程性有很大的想象空间, 这个方向的探索也非常重要, 但很可能是下一阶段的工作。

## 参考文献

---

- 1 Committee on Payments and Market Infrastructures. Digital currencies. Bank for International Settlements. 2015. <https://www.bis.org/cpmi/publ/d137.pdf>
- 2 Interview with Zhou Xiaochuan — Zhou Xiaochuan, the governor of the central bank, talking about RMB exchange rate reform, macro prudential framework and digital currency. Caixin Weekly, 2016, 6: 52–61 [专访周小川 —— 央行行长周小川谈人民币汇率改革、宏观审慎政策框架和数字货币. 财新周刊, 2016, 6: 52–61]
- 3 Broadbent B. Central banks and digital currencies. 2016. <http://www.bankofengland.co.uk/publications/pages/speeches/2016/886.aspx>
- 4 Fan Y F. Theoretical basis and structural selection of China's digital fiat currency. China Finance, 2016, 17: 10–12 [范一飞. 法定中国数字货币的理论依据和架构选择. 中国金融, 2016, 17: 10–12]
- 5 Yao Q. Consideration on China's digital currency design. China Finance, 2016, 12: 26–27 [姚前. 中国版数字货币设计考量. 中国金融, 2016, 12: 26–27]
- 6 Yao Q. Digital currency and bank account. Tsinghua Financ Rev, 2017, 7: 63–67 [姚前. 数字货币和银行账户. 清华金融评论, 2017, 7: 63–67]
- 7 Koning J P. Evolution in cash and payments: comparing old and new ways of designing central bank payments systems, cross-border payments networks, and remittances. R3 Reports. 2017. <https://www.r3.com/research/#toggle-id-14>

- 8 Bordo M D, Levin A T. Central bank digital currency and the future of monetary policy. NBER Working Paper 23711, 2017. <http://www.nber.org/papers/w23711.pdf>
- 9 Bech M L, Garratt R. Central bank cryptocurrencies. BIS Quarterly Review, 2017. [https://www.bis.org/publ/qrtrpdf/r\\_qt1709f.htm](https://www.bis.org/publ/qrtrpdf/r_qt1709f.htm)
- 10 Yao Q. Theoretical and technical logic of legal digital fiat currency. *Comp Stud*, 2017, 4: 179–196 [姚前. 法定数字货币的理论与技术逻辑. *比较研究*, 2017, 4: 179–196]
- 11 Yao Q, Tang Y W. Some thoughts on central bank digital currency. *Financ Res*, 2017, 7: 78–85 [姚前, 汤莹玮. 关于央行数字货币的若干思考. *金融研究*, 2017, 7: 78–85]
- 12 Yao Q. Conceptual prototype of Chinese digital fiat currency. *China Finance*, 2016, 17: 13–15 [姚前. 中国法定数字货币原型构想. *中国金融*, 2016, 17: 13–15]
- 13 Chaum D. Blind signatures for untraceable payments. In: *Advances in Cryptology — Crypto 82*. Berlin: Springer, 1983. 199–203
- 14 Dai W. B-Money. 1998. <http://www.weidai.com/bmoney.txt>
- 15 Jakobsson M, Juels A. Proofs of work and bread pudding protocols. In: *Proceedings of Conference on Communications and Multimedia Security*, Leuven, 1999. 258–272
- 16 Szabo N. Bit gold unenumerated: an unending variety of topics. 2008. <http://unenumerated.blogspot.com/2005/12/bit-gold.html>
- 17 Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2008. <https://bitcoin.org/bitcoin.pdf>
- 18 Project Jasper. A canadian experiment with distributed ledger technology for domestic interbank payments settlement. Report. 2017. <https://www.payments.ca/about-us/news/payments-canada-bank-canada-and-r3-release-detailed-findings-blockchain-experiment>
- 19 Monetary Authority of Singapore. The future is here — project Ubin: SGD on distributed ledger. 2017. <http://www.mas.gov.sg/singapore-financial-centre/smart-financial-centre/project-ubin.aspx>
- 20 Hong Kong Monetary Authority. Whitepaper on distributed ledger technology. Report. 2016. [http://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper\\_On\\_Distributed\\_Ledger\\_Technology.pdf](http://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf)
- 21 European Central Bank and Bank of Japan. Payment systems: liquidity saving mechanisms in a distributed ledger environment. Report. 2017. [https://www.ecb.europa.eu/pub/pdf/other/ecb.stella\\_project\\_report\\_september\\_2017.pdf](https://www.ecb.europa.eu/pub/pdf/other/ecb.stella_project_report_september_2017.pdf)
- 22 Yao Q. Development and supervision of digital currency. *China Finance*, 2017, 14: 38–42 [姚前. 数字货币的发展与监管. *中国金融*, 2017, 14: 38–42]
- 23 Danezis G, Meiklejohn S. Centrally banked crypto-currencies. 2016. <http://www.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf>
- 24 Yao Q. Central bank encrypto-currency — analysis of RSCoin system. *Caijing Weekly*, 2017, 13: 20–22 [姚前. 中央银行加密货币 —— RSCoin 系统之分析. *财经*, 2017, 13: 20–22]
- 25 Yao Q, Li L S. Application of big data analysis in digital currency. *China Finance*. 2016, 17: 37–38 [姚前, 李连三. 大数据分析在数字货币中的应用. *中国金融*, 2016, 17: 37–38]
- 26 Yao Q. The application of digital currency in interbank cash transfer scenario. *Finance Comput*, 2017, 5: 16–19 [姚前. 数字货币在跨行调款场景的应用研究. *金融电子化*, 2017, 5: 16–19]
- 27 Xu Z, Yao Q. The preliminary plan of digital commercial paper trading platform. *China Finance*, 2016, 17: 31–33 [徐忠, 姚前. 数字票据交易平台初步方案. *中国金融*, 2016, 17: 31–33]
- 28 Stiglitz J E. Macro-economic management in an electronic credit/financial system. NBER Working Paper 23032. 2017. <http://www.nber.org/papers/w23032.pdf>

## Understanding central bank digital currency: a systemic framework

Qian YAO

*Institute of Digital Money of the People's Bank of China\*, Beijing 100088, China*

E-mail: yaoqian@pbc.gov.cn

\* This article does not represent the opinions of the author's organization.

**Abstract** The rapid development of digital currency has raised big concerns among policy makers, regulators, industry and academia about the future of fiat currency. Increasingly the issuance of legal digital currency or digital fiat currency (DFC) is interesting central banks all over the world. However, what digital fiat currency should central banks need still remains obscure and need to be more deeply explored. This paper analyzes the essence and connotation of the legal digital currency from four dimensions — value connotation, technical means, implementation means and application scenarios. It is argued that DFC is a credit-based currency from a value perspective, a crypto-currency from a technical perspective, and algorithm-based currency in terms of its implementation and a smart currency when it comes to application scenario, these characteristics will enable DFC to excel over existing tools of electronic payment, be it private digital currency or electronic currency. DFC in China is expected to contribute to more stable value, more secure data, more powerful regulation, stronger empowerment of individuals in payment activities and smarter application and it can not only provide new tools for macroeconomic control but also lay a solid foundation for RegTech development and application.

**Keywords** digital fiat currency, credit-based currency, crypto-currency, algorithm-based currency, smart currency



**Qian YAO** was born in 1970. He is vice director-general of Technology Department of the People's Bank of China (PBC), head of Institute of Digital Money of PBC and the current secretary-general of China Financial Standardization Technical Committee. Holding a Ph.D. in engineering, he is a professorate senior engineer. Before joining PBC in 2010, he had worked at Information Statistics Department and

IT Service Center of China Securities Regulatory Commission and China Securities Depository and Clearing Corporation. During his time in PBC, Dr. YAO served as vice director-general of Credit Reference Center and member of Academic Committee of the Center for postdoctoral studies of Financial Research Institute and Credit Reference Center of PBC.