FRONTIERS OF
DIGITAL MONEY RESEARCH

数字货币研究前沿

第一辑

主编◎姚前

中国金融出版社

数字货币研究前沿

（第一辑）

姚　前　主编

中国金融出版社

责任编辑：陈　翎
责任校对：孙　蕊
责任印制：张也男

图书在版编目（CIP）数据

数字货币研究前沿（第一辑）（Shuzi Huobi Yanjiu Qianyan）/姚前主编. —北京：中国金融出版社，2018.6
ISBN 978-7-5049-9505-6

Ⅰ.①数…　Ⅱ.①姚…　Ⅲ.①电子货币—研究报告—中国　Ⅳ.①F832.46

中国版本图书馆 CIP 数据核字（2018）第 053724 号

出版发行　中国金融出版社
社址　北京市丰台区益泽路 2 号
市场开发部　（010）63266347，63805472，63439533（传真）
网上书店　http://www.chinafph.com
（010）63286832，63365686（传真）
读者服务部　（010）66070833，62568380
邮编　100071
经销　新华书店
印刷　北京市松源印刷有限公司
尺寸　169 毫米×239 毫米
印张　24
字数　305 千
版次　2018 年 6 月第 1 版
印次　2018 年 6 月第 1 次印刷
定价　65.00 元
ISBN 978-7-5049-9505-6
如出现印装错误本社负责调换　联系电话（010）63263947

前　言

纵观历史发展脉络，货币从早期的实物货币、商品货币到后来的信用货币，经历了多次形态演变。进入21世纪，建立在现代数字技术基础之上的数字货币呼之欲出，有望成为数字经济的主流货币形态，因此也吸引了世界各国的竞相探索与研究。根据职责要求，中国人民银行数字货币研究所具体承担数字货币与金融科技的研究、交流与合作职能，并在总行统一领导下开展央行数字货币的研发工作。

围绕研发工作中涌现的关键共性问题，聚焦数字货币与金融科技学科前沿，及时破解问题和固化科研成果，为总行相关工作提供决策参考，数字货币研究所创设了《研究专报》制度。自创设以来，《研究专报》从研究选题、研讨、行文、成果转化等方面，均得到了周小川行长、范一飞副行长等行领导的深切关怀和悉心指导，也得到了总行各部门的帮助和肯定。应各方要求，现将2017年《研究专报》中可以公开的研究成果汇编成《数字货币研究前沿（第一辑）》，以供参考并冀批评指正。

《研究专报》的定位是“顶天立地，包容并蓄，及时有效，知行合一”。“顶天”是要有国际领先的视野和站位，“立地”是注重把研究成果与实际工作紧密结合。“包容并蓄”是充分借鉴吸收国际央行以及产学研用各界的研究成果。“及时有效”则是对《研究专报》工作时效性的要求，做到及时乃至实时跟进评估相关理论、技术与政策进展。

最后，数字货币理论研究是认识的过程，是“知”，数字货币研发与相关政策出台是实践的过程，是“行”，唯有通过知行合一，把认识和实践统一，才能做好并不断提高《研究专报》的质量，发挥《研究专报》的智力支撑功能。

回首一年的研究实践，《研究专报》可以概括为以下几个主题：

一是央行法定数字货币理论体系研究。这部分研究关注的是央行数字货币的系统框架和总体设计，对于数字货币体系设计中的关键要素进行分析梳理，阐述央行数字货币的形态范畴、实现路径以及发行影响等问题，读者从中可以更加全面了解和深刻认识央行数字货币的本质内涵。

二是央行法定数字货币应用场景研究。应用场景是数字货币的应用着力点和设计驱动力，应用场景研究部分深入调查研究了央行数字货币可能的典型应用场景，探讨数字货币应用于具体业务场景的实现模式、功能及业务技术特点，以及可能会产生的影响，为读者理解数字货币的应用意义提供了具象化感知。

三是各国央行数字货币试验的跟踪研究。他山之石，可以攻玉。目前，世界主要央行纷纷开展法定数字货币试验，数字货币研究所在与各国央行保持着常态化交流的同时，也在积极跟踪各国试验进度。这一部分梳理了世界上主要央行对法定数字货币的探索，分析总结各国央行在技术手段、机制设计和法律法规等方面取得的阶段性成果与结论，为我国央行数字货币的研发提供借鉴。

四是虚拟货币观察监测。2017 年以来，虚拟货币尤其是首次代币

发行融资乱象丛生，研究所一直对虚拟货币相关发展状况进行观察监测，为总行的监管工作提供工作支撑。这部分内容编译了国外金融监管部门发布的虚拟货币相关法律法规，也对虚拟货币和首次代币发行融资做出了我们的研究分析和判断，以供参考。

五是分布式账本技术。分布式账本技术是作为支撑加密货币的底层技术架构出现的，但其影响力已经拓展到货币金融、社会组织、计算机科学、信息安全、财务会计等多个领域，为央行数字货币技术架构提供了多方面的有益借鉴。这一部分对当前主流分布式账本技术架构进行了全面的研究和比较，并从传统分布式系统视角研究技术的演进趋势。

六是金融科技。金融科技是由科技进步驱动的金融创新，发展金融科技有助于金融普惠，也是增强金融服务实体经济能力的重要依托，已成为各国金融监管者聚焦的着眼点和发力点。这部分内容包含了该领域的国际动态以及我们对相关技术的研究和分析。

《数字货币研究前沿（第一辑）》是中国人民银行数字货币研究所2017年工作成果的浓缩，谨以此书向关切、关心中国人民银行数字货币研究所发展的诸位领导和同仁进行汇报，并致以鸣谢！期待与大家继续为中国法定数字货币和金融科技的发展而努力。若能引发各方的积极思考与探索，实乃幸事。

“大胆假设，小心求证”，应是研究该有的严谨态度，鉴于这个领域的快速发展，书中难免有不足与错误，希请方家指正。

目　录

央行法定数字货币理论研究

央行法定数字货币应用场景研究

各国央行法定数字货币试验

虚拟货币观察监测

分布式账本技术

金融科技研究

央行法定数字货币理论研究

◇ 理解央行数字货币：一个系统性框架

◇ 数字货币与银行账户

◇ 关于央行数字货币的若干思考

◇ “去现金化”与现金的未来

◇ CPK 户币———法币的数字化

◇ 数字基础货币：来自欧洲央行的评估

◇ 数字货币对央行货币政策调控的影响

◇ 国际电信联盟数字法币网络基础设施焦点组工作草案

理解央行数字货币：一个系统性框架

姚　前

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、应用场景四个全新的维度，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。

一、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（Committee on Payments and Market Infrastructures，CPMI）将法定数字

货币定义为加密货币（crypto - currency）[①]。随后，中国人民银行行长周小川提出数字货币可分为基于账户和不基于账户两种[②]。继 Broadbent[③] 提出央行数字货币（Central Bank Digital Currency，CBDC）的概念后，中国人民银行副行长范一飞[④]指出央行数字货币主要属于现金（M0）范畴。中国人民银行数字货币研究所所长姚前[⑤]则提出了基于账户（account - based）和基于钱包（wallet - based）的数字货币概念，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[⑥]，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，复用现有成熟的金融基础设施，避免狭义银行化影响。与之相似，Koning[⑦] 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[⑧] 将法定数字货币区分为 CBDC 账户和 CBDC 代币。而 Bech 和 Garratt[⑨] 则提出央行加密货币（Central bank crypto currencies，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）四个角度对 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

① Committee on Payments and Market Infrastructures. Digital currencies. Report. 2015.

② 周小川．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 [cited 2016]. Available from: http://www.bankofengland.co.uk/publications/pages/speeches/2016/886.aspx.

④ 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 姚前．中国版数字货币设计考量．中国金融，2016a，12：26 - 27.

⑥ 姚前．数字货币和银行账户．清华金融评论，2017a，7：63 - 67.

⑦ Koning JP. 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.

⑧ Bordo M D, Levin A T. Central bank digital currency and the future of monetary policy. NBER Working Paper No. 23711. 2017.

⑨ Bech M, Garratt R. Central bank Cryptocurrencies, BIS Quarterly Review. 2017.

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、实现手段和应用场景四个全新的维度，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。

二、法定数字货币在价值维度上是信用货币

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。这使其天生就具有私人数字货币无法比拟的优势。

（一）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。对于货币的价值贮藏功能，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。布雷顿森林体系崩溃以后，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乌托邦情怀，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，在交易费用上也不具有明显优势，这些缺陷决定了其难以成为真正的货币。

（二）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、门格尔、瓦尔拉斯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，它们只是覆盖在实物经济上的面纱，对经济无实质性作用，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。凯恩斯主义者、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，每四年产生的数量减半，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，可以通过提高中央银行独立性来解决。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法定货币的价值稳定。

三、法定数字货币在技术维度上是加密货币

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；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。

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[①] 最早提出一种具有匿名性、不可追踪性的电子现金系统。Dai[②] 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[③] 提出工作量证明机制。Szabo[④] 发明了 Bitgold。Nakamoto[⑤] 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型，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

① Chaum, D. Blind signatures for untraceable payments. Advances in Cryptology, proceedings of Crypto, 1983, 82: 199 - 203.

② Dai, W. B - Money [cited 1998]. Available from: http: //www. weidai. com/bmoney. txt.

③ Jakobsson M, Juels A. Proofs of work and bread pudding protocols. Springer US, 1999, 61: 53 - 56.

④ Szabo, N. Bit Gold unenumerated: an unending variety of topics. [cited 2008]. Available from: http: //unenumerated. blogspot. com/2005/12/bit - gold. html.

⑤ Nakamoto, S. Bitcoin: a peer - to - peer electronic cash system [cited 2008]. Available from: https: //bitcoin. org/bitcoin. pdf.