

· 国外经济理论动态 ·

数字货币理论与实践研究进展^{*}

李建军 朱烨辰

内容提要:近年来,随着区块链、大数据与云计算等金融科技的发展,数字货币创新并快速发展成为世界各国关注的焦点,许多国家的中央银行正在积极研究发行主权数字货币相关技术的可行性,这推动了数字货币的理论与实践进入繁荣发展阶段。本文对数字货币的技术与实践源流、理论模式演进与实践进展脉络进行了梳理,试图归纳出数字货币的演进规律和趋势,分析数字货币对主权国家以及全球金融体系可能产生的影响。本文认为,技术推动了货币形态的演进和创新,数字货币本身属于信用货币,必须由中央银行控制发行;未来中央银行发行的主权数字货币可能作为一种补充性法定货币;同时货币当局要加强对私人数字货币的规范和监管,由于其不具有公信力,投机性强,应将其应用严格控制在局部范围之内,对于利用私人数字货币进行的非法融资活动要坚决取缔。

关键词:央行数字货币 私人数字货币 虚拟货币 区块链技术

伴随着区块链技术的应用,数字货币逐步替代原网络虚拟货币,出现了快速发展的势头,由此,数字货币的属性、定位、规制等问题引发了金融业界和学界的广泛讨论。2009—2017年间,数字货币由小到大,特别是在近两年中,全球数字货币种类与规模快速膨胀,一些国家和地区出现了利用私人数字货币开展非法融资的现象,给主权货币运行与金融监管带来了新的挑战。那么,如何看待数字货币现象,理论界的研究进展到什么程度?以中国人民银行为代表的全球主要央行开展的主权数字货币实践探索有何现实意义?本文将试图回答以上问题。我们首先对数字货币的理论文献以及世界主要国家的数字货币实践技术与规制建设进行梳理,归纳总结出数字货币理论与实践的发展状况;之后探讨数字货币给主权国家和全球金融体系带来的影响;最后对数字货币研究领域进行总结,分析数字货币实践研究的方向。

一、数字货币发展源流与理论归纳

2013年以来,国内外研究数字货币的理论文献开始增多。最初,大部分文献聚焦于讨论比特币(Bitcoin)的属性和其价格变化上,分别从理论和技术角度研究比特币是否具有货币属性,比特币的价格波动特征等。近年来,随着多国央行着手研究主权数字货币的发行技术、模式和制度等关键问题,学术界开始从央行数字货币的实践层面分析未来数字货币的发展方向。那么,数字货币与传统货币相比较,其出现和发展与哪些因素有关呢?

从货币史的角度看,货币起源于人类商品交换过程,货币形态的演进正是在不断适应着交换过程便捷性的基本需要中,逐步从有价值的实物货币转向了依靠国家主权担保的无内在价值的信用货币。在货币形态演进过程中,科技的发展起到了重要支撑作用,货币形态的每一次演变都伴随着技术的重大进步。从商品货币到金属货币,得益于冶炼技术进步;从金属货币到纸质货币,是造纸与印刷技术推动的;从纸质实体货币到电子货币,是计算机技术的应用体现。今天的数字货币与互联网、

^{*} 李建军、朱烨辰,中央财经大学金融学院,邮政编码:100081,电子邮箱:ljlsh@126.com,yczhu@163.com。基金项目:国家社科基金重大项目(14ZDA044)。感谢匿名审稿人的修改建议,文责自负。

云计算、区块链等技术的应用有直接关系。

(一)数字货币的形式演变与技术进步的关系

数字货币不是凭空出现的,它源自于电子支付,由电子货币、虚拟货币演化而来,并逐渐与电子货币和网络虚拟货币分离。学术界普遍认为电子支付发源于荷兰,在20世纪80年代末期,荷兰偏远地区的加油站经常发生抢劫现金的事件,安保人员工作危险大,而且对于加油站来说聘用成本过高。后来,有人将钱储存在新型智能卡上,提供给卡车司机消费,避免了卡车司机使用现金从而面临被抢劫的风险。与此同时,荷兰当时最大的零售商 Albert Heijn 推动银行发明了一种新的支付方式,可以让购买者直接用银行账户来支付,这就是现在 POS(point of sale)机的前身。在电子支付的依托下,部分学者和研究机构持续开展了对数字货币的理论探索和实践应用的研发工作。

Chaum(1983)首先提出了电子货币的概念,并在其论文中构造了一个具有匿名性、不可追踪等特性的货币系统,该系统被认为是最早的数字货币方案,其构造原理采用了密码学技术——盲签名。盲签名技术可以使签名者在不获取所签署具体内容信息的情况下完成签名。在该电子货币方案中,货币发行方使用盲签名技术对付款方的支付信息进行签名,签名后付款方可以进行验证,并将支付信息发往收款方完成收款,从而实现了电子货币的匿名性和不可追踪性。由此,密码学的原理和方法可被认为是构造电子货币系统的基础。Chaum 随后创建了 DigiCash 公司,并将其技术产业化为 E-cash 系统。这种不可追踪的现金引起了媒体前所未有的关注。但是,E-cash 系统采用中心化的架构,从而导致了其应用范围较小,一旦中心化的公司、中央服务器崩溃,该系统就不可维持。

随着近30年来密码技术的发展,数字货币方案也得到了不断优化。主流数字货币大致分为两种类型:一是在 E-cash 系统基础上进行扩展的未使用区块链技术的数字货币,二是以比特币的诞生为起点,使用区块链技术的分布式记账数字货币。1996年出现的 E-gold 电子货币系统完全独立于常规金融机构,E-gold 软件保证支付过程的安全和高效。E-gold 的发明者力求创建一个私人黄金货币体系,包括基于互联网的交易,其表现优于国家货币(Mullan,2014)。然而 E-gold 最后演化成为一种被犯罪分子利用的传销手段,已经被各国政府封杀。1997年,Adam Back 发明了 HashCash,用到了工作量证明(PoW)(Back,2002)。Szabo(1998)所发明的 BitGold,利用 PoW 将困难问题解答结果用加密算法串联在一起公开发布,构建出一个产权认证系统。Dai(1998)提出了匿名的、分布式电子现金系统:B-money。1998年还曾出现过两个生命十分短暂的数字货币:BEENZ 和 FLOOZ,二者十分相似,它们都声称将创造一种用于网络消费的统一货币,并且将挑战传统货币。然而,在与信用卡的竞争中,它们败下阵来,在2001年宣布失败。在比特币出现之前的所有数字货币中,Q币比较特殊,它一开始是作为腾讯公司开发的仅能用于购买腾讯内部虚拟商品和服务的虚拟货币被大家熟知的。但是随着 Q 币被越来越多人接受,许多线下的商品和服务也开始接受 Q 币支付,Q 币的使用范围大大超越了虚拟货币的范畴。随之而来的是,市场的混乱和被不法分子的利用,使得 Q 币最终被政府限制了使用范围,恢复了虚拟货币的身份。

然而,数字货币在这一阶段的探索很多只限于纸面设计,少数付诸实施的系统也均以失败告终,要么根本没有流通,要么流通的范围极其有限。失败的原因大多可归结为中心化的组织结构。在缺乏国家信用支撑的情况下,一旦发行和维护组织破产或遭受法律、道德指责,或保管总账的中央服务器被黑客攻破,这些货币系统将面临信用破产与内部崩溃的风险。如果不使用中心化的组织结构,那么如何对数字货币的流通进行监管就成了一个棘手的问题。数字货币也容易遭受复制和篡改,而且数字货币在网络中的流通记录最终必然要记录于某个“账本”中,如果遭受黑客攻击和篡改,则将带来毁灭性的破坏。因此,要保障数字货币系统的安全性,需要解决两个问题:(1)避免货币伪造;(2)避免双重支付,即利用货币的数字特性两次或多次使用“同一笔钱”完成支付。早期的数字货币也曾在这两个问题上进行了尝试,归纳起来看,B-money 是一种匿名的、分布式电子现金系统,使用工作量证明机制发行数字货币,通过网络广播交易信息并进行真实性证明,解决伪造货币和双重支

付的问题(Dai,1998)。BitGold 方案也是采用工作量证明的方法解决货币伪造和双重支付问题(Szabo,1998)。在 DigiCash 方案中,首次在数字货币中引入了密码学方法,使用了盲签名算法切断了货币提现与支付之间的联系(Chaum,1983)。

之后的数字货币技术又有了新的发展。Nakamoto(2008)在密码学邮件组发表了一篇论文,提出了比特币的概念。Nakamoto 认为,借助金融机构作为可信赖的第三方来处理电子支付信息,受制于“基于信用的模式”(Trustbased Model)的弱点,因此希望创建一套基于密码学原理,使得任何达成一致的双方不需要第三方中介参与,能够直接进行支付的电子支付系统,该系统能够杜绝伪造货币和双重支付。比特币的核心支撑技术是区块链,其主要特点是去中心化,能够通过运用数据加密、时间戳、分布式共识和经济激励等手段,在节点无须互相信任的分布式系统中实现基于去中心化信用的点对点交易、协调与协作,从而为解决中心化机构普遍存在的高成本、低效率和数据存储不安全等问题提供了一种可选的解决方案。比特币是一个开源项目,其源代码也作为其他的一些软件项目的基础。由比特币衍生出来的最常见的形式,就是替代性的去中心化货币,简称“竞争币”,这类货币使用了跟比特币相同的模式,创建区块链来构建自己的电子货币系统。竞争币中较为知名的有莱特币(Litecoin)、狗狗币(Dogecoin)、点点币(Peercoin)、门罗币(Monero)、达世币(Dash)等。

从上述货币发展以及数字货币的源流分析,我们可以归纳出数字货币发展演变的决定因素,表示成四元组模型:DF=f(T,A,P,L)。其中,T 表示技术(Technology)条件,数字货币是伴随着信息技术的发展而产生与发展的。正是由于互联网的普及和发展,分布式网络、云计算等技术的普及,才有了区块链技术,才有了工作量证明和比特币的出现,才有了更多形式的数字货币。A 代表应用(Application)需求,数字货币的发展是由应用需求驱动的,实践探索出的经验对数字货币的发展起到了关键性的作用。P 代表支付环境(Payment),数字货币的发展与支付环境密切相关,数字货币与电子支付、移动支付的发展密不可分,是数字货币发展的前提条件之一。L 表示法制(Law),数字货币的发展受到法规制度与政策环境的影响,从各国政策对比特币价格的影响可以看出,法规制度与政策环境能够显著影响数字货币的发展。

(二)数字货币内涵的拓展:官方定义与学者观点

关于数字货币内涵的界定,也是一个伴随实践发展逐步深化认知的过程。在数字货币之前出现的类似概念是电子货币(Electronic Money),之后出现了虚拟货币(Virtual Currency)和数字货币(Digital Currency),此时的数字货币仅仅是指利用数字技术承载的交易媒介。在数字货币概念的基础上,衍生出了加密数字货币(Cryptocurrency),成为目前数字货币的主流概念。各国央行的研究报告对数字货币的相关概念给出了官方注解,学者们在相关研究中或沿用央行的解释,或对央行的定义进行修正与拓展。目前,对数字货币、电子货币和虚拟货币内涵经常交叉混合。

从世界主要央行对数字货币的研究来看,欧洲中央银行(European Central Bank)最早定义了虚拟货币。其定义虚拟货币为不受监管的数字货币,同时,定义电子货币和商业银行存款为受监管的数字货币,等同于法定货币。加密数字货币则是除了受监管的数字货币和不受监管的数字货币之外的第三类数字货币(European Central Bank,2012)。英格兰银行 2014 年第三季度的报告(Robleh et al,2014)明确以分布式记账技术作为数字货币的分类标准,一类是加密数字货币,即运用分布式记账技术生成的数字货币,并指出比特币是史上第一个加密数字货币;另一类是非加密数字货币,典型代表有瑞波币(Ripple)。法国金融行动特别工作组(FATF,2014)定义虚拟货币为以数据形式表现的交换媒介、记账单位、价值储存等,但它不是法定货币,没有任何货币当局为其提供担保。电子货币则与之不同,是法定货币的电子形式。数字货币则代表了虚拟货币(即非法定货币)和电子货币(即法定货币)的总和。Barrdear & Kumhof(2016)在英格兰银行的工作论文中,将中央银行数字货币定义为通过分布式分类账实施的普遍认可且有息的中央银行负债,与同为交换媒介的银行存款相

竞争。

目前学术成果中对数字货币内涵进行明确定义的并不多,大多数学者直接沿用了各国政府发布的定义,一部分学者对数字货币的内涵进行了讨论和拓展。Wagner(2014)将数字货币定义为以电子形式储存和转移的货币。这一定义较为笼统,不仅包含了数字货币,还包含了电子货币在里面。Dwyer(2015)从功能视角讨论了数字货币的内涵,认为数字货币最关键的问题是防止双重支付问题,比特币的点对点支付系统在一定程度上可以解决该问题。Bissessar(2016)借鉴英格兰银行的定义,明确提出数字货币是去中心化的运用分布式记账系统的货币,例如比特币、莱特币、狗狗币等。这一定义将没有采用分布式记账系统的诸如瑞波币等产品排除在外。Kraus(2017)认为数字货币包括虚拟货币和加密数字货币,而虚拟货币和加密数字货币的区别是,虚拟货币仅在特定的虚拟空间内流通,而加密数字货币则打通了虚拟和现实的界限,可以在现实中购买商品或服务,可以与现实中的货币相互兑换。加密数字货币的另一个重要特征是采用分布式记账,实现了去中心化,没有管理者管理其发行和运营。

本文认为,数字货币可以区分为宽口径数字货币和窄口径数字货币。宽口径数字货币包括电子货币,属于主权法定货币的数字化;虚拟货币是私人发行的在特定网络范围使用的支付手段;加密数字货币包括央行发行的主权数字货币与私人发行的去中心化的数字货币。窄口径数字货币专指加密数字货币,中央银行发行的主权数字货币是真正意义上的货币,有主权信用担保;私人发行的加密数字货币,由于缺乏信用,容易被操控,投机性强、竞争无序,无法成为价值稳定的数字货币,难以归入真正意义上的流通计价和储值货币。

(三)数字货币的理论归纳

货币理论阐释了货币的起源、属性、形态演进、规制设计等基本规律,数字货币作为货币体系发展演进到后现代化阶段的产物,与以往的货币形态相比具有特殊性,但又继承了货币的内涵与发展规律。它在以下三方面拓展了货币理论的范围:(1)主权数字货币是货币演进的主要形式。数字货币作为货币只能走向主权数字货币形式,私人数字货币只是一种超越网络虚拟应用范围的有限支付工具,如果长期缺乏规制政策环境的支持,其生命力不可能维持长久。而中央银行基于现代科技发行的主权数字货币,具有现代货币的本质属性,那就是国家主权的背书,其具有广泛的可接受基础,也具有持久的公信力。(2)数字货币较之非数字货币具有支付效率与行为约束力的先天优势,这一优势来自于现代金融科技的应用与支持,如区块链技术、深度学习与交互学习应用、人工智能技术等。主权数字货币的应用一定程度上可以防控社会经济活动中的道德风险,抑制黑色经济、腐败、经济犯罪等问题。在这方面,私人数字货币不具有这一优势。(3)数字货币运行需要建立在现代国家金融制度与国际金融规则之下,货币法规、制度与政策等环境是确保数字货币稳健运行的基础条件。尽管说技术在一定程度上可以替代制度功效,但不能取代制度,制度设计是货币运行的生态要素,技术是保障基础。因此,数字货币必然要以主权货币形式发展,非主权的私人信用货币,由于不具有主权信用,其价值的不稳定决定了其难以成为真正意义上的货币。另外,数字货币带来的现代货币体系变革,也需要我们构建起相应的理论研究分析框架。

结合以上对数字货币、电子货币和虚拟货币的讨论,本文对数字货币相关理论认知问题归纳如下:按照窄口径数字货币界定,它是以加密数字形式存在于网络空间的、可以行使货币职能的可监管的交换媒介。从发行方式、流通范围和与法定货币的关系来看,这三者之间有显著的不同,从出现的时间来看,它们之间相互承接,互相启发。电子货币出现最早,在电子支付应用之后,主权货币电子化便是电子货币。随着第三方支付的出现,电子货币的范围从金融机构拓展到非金融机构。虚拟货币是随着虚拟社区的问世而出现的,它实际上并不是货币,而是虚拟商品的一种,可以在指定范围内兑换虚拟商品和虚拟服务。数字货币的概念则不同于前两者,它是一种以数字符号表示的能够在国际范围内流通的交换媒介。数字货币与电子货币的区别是,发行和流通是否与法定货币挂钩;数字货币与虚拟货币的区别是,流通范围不仅仅局限于虚拟空间,而是可以在现实世界流

通,甚至可以跨境流通。从虚拟货币、电子货币、数字货币的概念中,我们能够归纳出数字货币发展的基本路径。

二、数字货币的实践研究进展

(一)数字货币发行:私人数字货币的研究进展

私人数字货币是以非国家为发行主体的数字货币,例如以企业信用背书发行的数字货币和无发行主体的去中心化数字货币等。不同主体发行的数字货币之间将形成竞争关系,为了检验竞争货币之间是否存在有效竞争,Fernández-Villaverde & Sanches(2016)建立私人货币竞争模型,从模型中并不能得出竞争性货币更加有效和稳定。但是,生产性资本的引入从根本上改变了模型的基本属性,所以,存在一个唯一的均衡分配,可以根据技术资本回报率任意地接近效率分配。该研究的意义在于,明确了有利于社会的私人货币体系的特征。私人数字货币能否打破主权货币的垄断局面?在19世纪至20世纪初期的北美曾出现“自由银行”(Free Banking),在这一政策之下,私有银行可以发行自己的货币,国家对货币发行没有垄断地位。货币自由发行的结果是带来更加严格的监管措施,在竞争环境中银行的频繁倒闭破坏了金融稳定,削弱了人们对纸币的信任。最终在20世纪初期,私人银行发行货币被禁止,只有国家拥有发行货币的权利(Frankel,1998)。

学者对私人数字货币的探讨主要分为两部分,一部分学者讨论了数字货币是否具有货币属性的问题,另一部分学者从数字货币市场的产品的特征研究数字货币的特点。在研究数字货币的文献中,目前研究比特币这一代表性数字货币的文献占比很大,尤其在2013年比特币价格大涨之后,对比特币市场特征、价格形成等方面的研究开始增多。

1. 私人数字货币的货币属性研究。比特币能否被称之为货币存在较大争议,Wallace(2011)、Grinberg(2011)认为比特币是一种高效率、低成本的价值交换方式,是理想的货币形式。Chowdhury & Mendelson(2014)认为在虚拟货币和金融体系的框架下,人们对于比特币类的虚拟货币的认可程度还需要以虚拟货币不断发现其内在价值作为依据。Swan(2015)为数字货币的职能划分了三个层次,从高到低分别是交换媒介、交易软件、记账工具。Glass(2016)援引Swan的划分,认为比特币在设计之初就是作为交换媒介,属于数字货币的最高层智能,所以比特币属于数字货币的范畴。但是更多的学者并不认可比特币的货币身份。Yermack(2013)的观点是,与其说比特币是一种货币,不如说是一种投机性工具。因为,一方面,比特币的每日汇率走势与其他主要货币汇率走势没有相关性,使得比特币无法用于风险管理目的,比特币的持有者也很难对比特币持有头寸进行套期保值;另一方面,比特币无法用来为消费信贷或其他贷款合同计价,也难以被纳入具有存款保险特征的银行体系。Šurda(2012)认为经济参与者之间的信任保证了比特币市场体系的稳定,但比特币既没有内在价值又没有代表性,它的价值取决于市场力量和使用者的信心。这表明比特币的价值是没有保证的,无法受到任何货币权威机构的支持,但同时这也意味着除了消费者信心,没有其他因素能够操控比特币的价值和供给。实际上,比特币的价值就来源于市场对比特币的信心。从这个角度而言,比特币与其说是一种货币,不如说是一种商品。Woo et al(2013)、Bouoiyour et al(2014)、Al-styne(2014)、Hanley(2015)研究了比特币的内在价值,他们一致认为比特币内在价值为0,其价值仅为纯粹的市场价值,是一种投机性商品。目前,大部分学者对以比特币为代表的私人数字货币的货币属性不予认同,只认为其属于数字商品或资产,是投机的工具。

2. 私人数字货币的市场特征研究。除以上讨论之外,研究比特币的大多数学者回避了讨论其货币属性,专注研究比特币市场的各方面特征,默认其为一种金融资产。其中,对于比特币市场有效性问题的研究目前仍没有定论。Brown(2014)通过检验对超额回报和市场流动性的预测能力,认为比特币市场存在短期价格可预测性,证实比特币市场不符合弱有效市场假说。Bartos(2015)运用误差修正模型分析比特币的价格特征,认为比特币遵循弱有效市场假说,其价格会立即对公开市场信息做出反应。Urquhart(2016)和Nadarajah & Chu(2017)对比特币的市场收益率序列进行了统计

分析,但二者得出了相反的结论。Urquhart(2016)的实证结果表明比特币市场还未达到弱有效市场,而Nadarajah & Chu(2017)改进了分析过程,得出了比特币市场已经符合弱有效市场假说的结论。Kurihara & Fukushima(2017)通过研究比特币的每周价格数据发现比特币市场的有效性越来越高,这就意味着比特币收益率在未来将越来越具有随机性。可以得出的判断是,随着时间的推移,比特币市场正在逐步完善,趋向于满足弱有效市场假说。在市场波动性检验方面,Ortisi(2016)、Bouri et al(2016)、Katsiampa(2017)等学者一致认为比特币市场波动性大,投机性高。Katsiampa(2017)测量了多个时间序列模型,认为AR-CGARCH是研究比特币数据最理想的模型。Donier & Bouchaud(2015)通过实证分析发现比特币价格的大幅下跌并不是由市场出现的新信息引起的,而是内生性循环的结果。他们认为这一结果可以为动态评估市场不稳定性和流动性风险预警提供依据,并且可能实现对市场崩溃现象的定量分析。Zhu et al(2017)用VCEM模型验证了影响比特币价格的若干宏观经济因素,认为宏观经济指标对比特币价格存在一定的影响。Cretarola & Talamanca(2017)认为市场信心对比特币价格有重要影响,他们建立了一个二元模型来描述比特币价格和信心因子之间的关系,并认为二者存在正相关性。

3. 关于ICO的研究。对于ICO(Initial Coin Offering 或 Initial Crypto-Token Offering),目前尚没有明确的定义,仅从字面来看,ICO显然是从IPO(Initial Public Offering)延伸而来,可以理解为首次数字货币代币发行。ICO已经成为区块链项目非常重要的融资手段。Chuen et al(2017)将ICO描述为基于区块链和加密数字货币的融资项目,投资人通过项目白皮书或其他文件评估项目价值并决定是否投资。Conley(2017)初步评估了ICO的可行性和定价等问题,并为创业者和投资者提出一些建议。

Conley对数字货币创始人提出了三点建议:(1)设计一个成功的代币必须参照货币理论、金融经济学、博弈论等理论,货币市场需要多方均衡,数字货币的使用率是增值的关键。(2)建议设计者为交易型数字货币设置以稳定数字货币价格为目的的基金。(3)创始人应注意,在ICO时不留存初始货币。多数ICO中存在最大的问题是,不管是营利性还是非营利性的公司,几乎所有公司的创办者都会留存一部分数字货币,大约占到总额的20%(瑞波币的创始人持有70%的瑞波币)。考虑到初创的数字货币只有一小部分流通,20%也代表了数倍的份额。特别是在卖出这些持有的原始币时,很可能被当作管理团队失去信心和套现的信号,或者该项目的成本远高于预期。所以,最好的做法是在ICO时卖掉所有的币,将收益的20%放入运营管理账户,或者其他需要使用的途径。

对于数字货币投资者,Conley也提出三点建议:(1)投资ICO以期其增值并不是一个良好的长期策略,交易型数字货币的价格建立在对未来价格的预期上,这种预期是十分脆弱的。(2)投资组合中数字货币价格的上涨并不能说明该投资的正确性,运气的成分很大,仍要警惕泡沫破裂的风险。(3)慎重投资那些名目不清、不完整或者根本不存在的白皮书,这可能意味着该项目不成熟或公司对投资人有所隐瞒,对于这样缺乏透明度的投资应谨慎。投资者应选择有明确收入来源的、公司拥有健全的营业模式和技术的数字货币项目。

ICO背后的金融诈骗问题已经引起各国的重视,美国、日本、加拿大等国政府金融监管部门也对ICO进行了风险警示,美国证券交易委员会拟将ICO纳入监管。与早期的E-GOLD类似,加密数字货币被非法利用,成为传销的手段,应该予以严厉打击。

(二)主权数字货币发行:中央银行数字货币的实践与研究进展

与私人数字货币市场的竞争不同,中央银行数字货币具有天然的发展优势。中央银行数字货币是国家结合自身货币发展需求,利用现有技术,以国家信用背书发行的货币,具有法定货币的性质。2016年1月20日,中国人民银行数字货币研讨会在北京召开,数字货币研究专家分别就数字货币发行的总体框架、货币演进中的国家数字货币、国家发行的加密电子货币等专题进行了研讨和交流,提出在前期工作的基础上继续推进,争取早日推出央行发行的数字货币。纵观世界各国,中央银行发行数字货币已经成为一种全球性的趋势,英国、加拿大、瑞典等国的中央银行也已经出台了发行自己

的数字货币的相关计划,欧盟中央银行也在考虑发行中央银行数字货币。

在央行数字货币的概念提出之前,Shoab et al(2013)就提出官方数字货币系统(Official digital currency system)的概念,这一概念和中央银行数字货币(Central bank digital currency)相似,即由央行或政府控制和发行数字货币。数字货币的发行方式与主权货币相同,但是控制系统完全不同。相比主权货币,数字货币更加安全、高效、便捷。较早出现的中央银行数字货币发行方案来自于Koning(2014)在博客中发表的题为“联储币”(Fedcoin,设想中的联储数字货币方案)的文章,其中详细描述了中央银行数字货币的发行方案。Fedcoin 可以允许个人和企业直接在中央银行开户,而不需要商业银行作为中介机构。私人数字货币去中心化的设计牺牲了价格的稳定性,在没有稳定的后备基础的情况下,诸如比特币等一类私人数字货币面临剧烈的价格波动,这种价格波动还具有强烈传导性。Fedcoin 可以解决价格波动这一难题,重新引入中央控制节点来管理货币系统,使央行可以在调节货币供给方面发挥作用。Fedcoin 保留了比特币去中心化以外的其他特征,同时还赋予中央银行纸币所没有的功能:负利率。Haldane(2015)就指出,中央银行数字货币可以解决利率“零下限”的问题,允许央行将利率降低至零以下,可以作为一种鼓励消费和投资的策略。Fedcoin 的思路也被英格兰银行借鉴。英国央行发行数字货币的目标有两点:一是创造一种交易更高效、透明度更高、成本更低的货币;二是为数字货币市场注入信心,同时对数字货币市场实行监管,解决现存的若干不良因素。Raskin & Yermack(2016)针对中央银行发行数字货币进行了拓展研究,他们认为,数字货币背后的区块链技术有可能改善中央银行的支付和结算业务,并可能成为中央银行推出自己的数字货币的平台;而且,主权数字货币可能对银行体系产生深远的影响,缩小了公民与中央银行之间的距离,减少了公众对商业银行存款的需求。本·布劳德本特(2016)分析指出,如果央行数字货币允许个人在央行直接开户,则意味着基础货币和货币乘数效应不再存在,央行数字货币成为一种结算货币,绕过银行间清算过程,实现点对点的资金转移,在这种情况下,央行数字货币将与商业银行存款形成竞争关系,可能导致银行存款流失,对现代金融体系的基础结构产生重要影响。数字货币竞争会削弱中央银行实施货币政策的能力。当央行不再作为货币发行的唯一主体,而是成为竞争者与其他中央银行和私人行为者竞争时,市场的供给和需求将决定哪些货币成为普遍接受的交换媒介。Raskin & Yermack(2016)表示,中央银行是在政治体制下运作的,法律制度保证了其发行的纸币的强制流通。这样的法律不要求当事人与中央银行货币签订合同,而是拒绝向不接受国家法定货币而使用其他交换媒介作为债务承付的当事人提供法律帮助。这就出现了格雷欣法则中的劣币驱逐良币。法律制度赋予了政府垄断货币的特权,允许其印制货币。如果没有这类法律,中央银行就仅仅是银行。日本银行也开始关注央行数字货币的发行,副行长 Nakaso(2017)认为央行数字货币一定程度上代替了纸币的角色,将影响中央银行支付结算系统的运作。发行央行数字货币将拓宽公众与中央银行的接口,假设央行数字货币可以完全行使与纸币相同的功能,这将导致所有人都能全年全天获得与中央银行的接口,中央银行将完全开放。央行数字货币的出现固然会对现有的货币体系形成挑战,但与此同时,也为经济发展提供了新的机遇。另外,央行数字货币在便利跨国结算方面也有显著优势,在跨国结算中往往会经过多层检查与验证,这一过程不仅耗费时间,还涉及了众多中介机构参与,增加了交易行为的不可控性。数字货币可以实现中央银行直接监督存款人的行为:一方面提高交易效率;另一方面有助于打击洗钱、逃税等行为(Raskin & Yermack, 2016)。总体来说,央行数字货币的发行对宏观经济有正向影响,英格兰银行的研究员 Barrdear & Kumhof(2016)运用 DSGE 模型,在符合金融危机前美国的框架中分析得出,由于实际利率、扭曲性税收和货币交易成本的减少,央行发行的数字货币如果占到国民生产总值的 30%,则可以永久性提高 3%的国民生产总值。同时,央行数字货币将作为货币政策工具,提高中央银行稳定经济周期的能力。

(三) 各国政府对私人数字货币的监管措施

随着比特币等数字货币的发展,许多国家基于其具体国情选择合适的监管举措。英国、美国、日本等一些国家以及欧盟积极探索监管规则与监管体系的建立,包括开展试点、立法支持、加强应用

等。2014年,英格兰银行发布了两份报告(Ali et al, 2014),称比特币是一种“商品”,是“真正的技术创新”。2016年3月,英国率先提出可由央行调控的法定数字货币原型系统——RScoin中央银行加密数字货币(Centrally Banked Cryptocurrencies),开启了由央行主导的数字货币研究工作。美国政府对比特币存在的风险进行了多次警示。2013年,美国反洗钱交易报告中心——金融犯罪执法网络(FinCEN)出台了有关虚拟货币的指导意见(VC Guidance)^①,指出比特币属于“可转化的虚拟货币”,应纳入反洗钱监管范围,受《银行保密法》监管。美国证券交易委员会(SEC)对比特币投资者给予风险预警。美国国税局(IRS)出台了适用于比特币和其他可转化货币的指导意见,将虚拟货币看作是一种需要缴纳联邦税的财产。2013年8月,德国宣布将比特币纳入国家监管体系,法国也提出任何比特币的交易平台必须通过法国央行的认证或者通过已注册的公司来留存平台交易的基金。2016年5月,日本国会批准有关加密电子货币的新法案,将加密电子货币交易所归到金融厅(FSA)下进行监管,要求由注册会计师对这些交易所进行审计。2014年,俄罗斯央行针对数字货币发表声明,指出比特币等数字货币“没有国家实体支持,投机性较强,其在相关虚拟交易中的交易具有高风险特征”(万晨,2016)。2015年,俄罗斯财政部制订了一项新的法律草案,将涉及数字货币的活动列为非法,并实行刑事处罚,个人发行货币替代品将会面临四年的有期徒刑。

总体来看,世界各国对以比特币为代表的私人数字货币多采用严格的监管态度,将其交易纳入现有的监管框架,适用相关监管法律法规。

三、中国数字货币理论与实践研究的进展

国内学者主要关注数字货币内涵、对央行数字货币发行及其对金融体系影响三方面,近年来也取得了一定的成果。

(一)对数字货币内涵的理解

国内学者对数字货币的认知是从虚拟货币开始的。贾丽平(2009)开始关注网络虚拟货币,并定义广义的网络虚拟货币为高科技中代替实体货币流通的信息流或数据流。狭义的网络虚拟货币具有支付功能,由各网络机构自行发行,不能实现现实的价值,不能通过银行转账,没有形成统一的发行和管理规范,只能流通于特定网络世界。随后,贾丽平(2013)进一步总结了比特币的五个特点:信息货币和私人货币的结合,不会发生通胀和通缩,高度匿名,使用方便,交易成本低廉。谢平等(2013)对电子货币的定义是,以虚拟账户代表货币价值,储存于电子装置,是发行机构及其密切商业伙伴以外的实体可以接受的支付手段。周光友(2015)将电子货币总结为:发行主体趋于分散,流通突破主权范围,交易更加隐秘,交易过程更加安全,交易成本更低。显然,谢平等人与周光友所定义的电子货币并不属于同一范畴。谢平等人的电子货币概念实际上与本文数字货币的概念较为一致。周光友对电子货币特点的总结也可以看作是私人数字货币的发展特点,尤其是发行主体趋于分散和流通突破主权范围两点。李志杰(2017)明确定义了基于区块链的数字货币,他认为,数字货币来自开放的共识算法,基于发行机构的发行策略或基于算法解得确定数量,需要经过网络中达到一定数量节点的认可,保证交易过程完整。这一定义较为全面地概括了目前出现的分布式记账数字货币的特征,并且包含了可能出现的央行数字货币。

(二)对央行发行主权数字货币的研究

国内学者对于央行发行数字货币大多持乐观看法,并且认为央行数字货币比私人数字货币更有发展空间。盛松成、蒋一乐(2016)就提出“只有央行发行的数字货币才是真正的数字货币”,只有中央银行对数字货币进行发行和调控,才能维持由国家信用支撑的现代货币体系的稳定。发行数字货币也将提升中央银行对货币发行和流通的控制力,加强货币政策的传导和运行。姚前(2016)也强调,不能狭隘地将数字货币理解为就是比特币,要区分法定数字货币与私有数字货币在技术特性、经济特性和制度安排上的异同和关联,讨论数字货币履行货币职能的过程,以及如何满足高质量货币体系的条件。张正鑫、赵岳(2016)认为央行发行数字货币具有很大优势,表现在,总量可控、可以降

低信用风险和具有公平性和非营利性。徐忠等(2016)借鉴以太坊创始人提出的完全开放、联盟、完全封闭三种可行系统的设想,为中央银行发行数字货币提出三种方案:(1)完全开放系统;(2)联盟系统;(3)完全封闭系统。这三种方案都是基于分布式账本技术的不同程度的应用。相对于传统货币,数字货币可以降低交易过程中的信息不对称,降低市场摩擦,提高交易的效率和质量。中心化的金融系统很难抵御黑客进攻,若采用区块链技术,具有全网记账、分布式等特点,则可以抵御一部分黑客的攻击。即使局部节点遭受攻击,全网各个节点中的交易数据仍然安全(李志杰,2017)。所以,央行数字货币不仅代表了一种新型货币,更是一种新型的记账系统。此外,比起中心化的货币体系,分布式账本保证了金融数据的安全性和完整性,可以降低洗钱、逃税、贪污等经济犯罪行为。就目前的发展来看,短期内数字货币难以成为主流货币体系替代现有货币体系,但是可能成为现有货币体系的良好补充。

(三)发行央行数字货币对金融体系的影响

数字货币仍处于动态的发展过程中,对央行数字货币的技术路线并未达成一致,目前普遍认可的形式有两种:一是央行直接发行数字货币,市场交易主体可以直接在央行开立账户;二是依旧遵循央行—商业银行的二元模式。但本文对数字货币与金融体系的关系的分析不局限于某一种数字货币框架。

首先,数字货币的发行意味着货币发行方式和结算方式的重大变革,将引发货币供求方式的改变。随着信息技术的发展,个人、企业、金融机构等主体之间的资金清算越来越多地由现钞清算转变为记账清算。记账清算可以降低流通成本,而且每笔交易都可追踪,可以降低交易风险,优化资源配置(王永利,2016)。数字货币将实现完全的记账式清算。在货币投放方面,如果央行数字货币仅作为电子现金的一种,用于减少部分实物现金的需求,将会令小额支付系统更高效,对货币政策和商业银行的影响并不显著(温信祥、张蓓,2016)。在货币结算方面,数字货币的应用将提高使用的便捷性,便捷程度的提高会使交易总量上升,提高整个经济体系的流动性、降低交易成本(徐忠等,2016)。从央行管理货币角度分析,法定数字货币会极大提升货币运行效率。

其次,数字货币作为一种补充性货币,其应用将直接影响货币政策传导与效果。补充性货币投放扩大了货币乘数,它对货币存量、货币流通速度和价格水平的影响取决于该种货币与法定货币的兑换方式(贝多广等,2013)。央行发行的数字货币本身就是法定货币,具有完全的兑换性。数字货币的技术创新无法完全取代中央银行货币发行和货币政策,但是,央行数字货币可以提升货币供给和货币政策的有效性。数字货币分布式记账功能使交易信息无法篡改,便于追踪资金流向,有利于货币当局准确灵活地运用货币政策工具,全面检测和评估金融风险;数字货币点对点的支付结算方式可以提高货币政策的传导效率,降低金融体系的利率水平,平滑利率期限结构,实现物价稳定和经济发展(盛松成、蒋一乐,2016)。从这个角度讲,法定数字货币推行有助于货币政策目标的实现。

最后,数字货币进入大规模运用之后,货币结构出现较大变化,原有货币运行机制会出现新的特征,可能引起金融市场波动,数字货币必然引发金融监管体系的革新。数字货币作为互联网金融发展中出现的新货币形态,对其进行统一的规范监管是必要的(刘澜飏,2013),所以由央行发行法定数字货币是一种必然选择。法定数字货币也将对金融体系带来一定的不确定性。一方面,法定数字货币可能会使货币结构发生变化,由于数字化,实物货币需求量下降,金融资产的转换速度加快。另一方面,法定数字货币会影响货币创造,在法定数字货币之下,存款货币向现金货币的转换更加快速,当金融危机出现时,金融恐慌和金融风险的传播速度也将加快,从而影响金融稳定(范一飞,2016)。所以,私人数字货币的监管,必须明确其地位和性质,引导为主,管制为辅。货币当局要为数字货币交易平台设立准入门槛,明确交易规则,促进数字货币的良性竞争,还要防止数字货币成为非法经济活动的工具(李志杰,2017)。监管方式可以采取小范围试点,取得经验后再行推广。不过,私人数字货币发行需要限定在一个合理范围之内。

(四)对私人数字货币的监管实践

比特币进入中国以后,对金融领域的影响越来越大,引发的投机活动造成了市场混乱。从一开始,中国人民银行对比特币的态度就十分谨慎,2013年12月下发的《关于防范比特币风险的通知》^②指出,比特币不是由货币当局发行,不具有法偿性与强制性等货币属性,并不是真正意义的货币,不能且不应作为货币在市场上流通使用,比特币交易是一种互联网商品的买卖行为。2014年3月,中国人民银行又下发了《关于进一步加强比特币风险防范工作的通知》,要求各银行和第三方支付机构关闭10多家境内比特币平台的所有交易账户。2017年9月,中国人民银行牵头的互联网金融工作组起草相关规则,禁止境内比特币和其他数字货币交易平台。

利用代币发行(ICO)进行融资在中国源于2015年,之后,ICO规模快速增长,到2017年上半年进入高潮阶段。由于缺乏监管,不少企业利用ICO进行集资诈骗,演化为传销闹剧,造成市场混乱,积聚了较大的风险。2017年9月4日,中国人民银行发布的《关于防范代币发行融资风险的公告》^③明确提出,国内通过发行代币形式包括首次代币发行(ICO)进行融资的活动涉嫌从事非法金融活动,严重扰乱了经济金融秩序,应当立即停止。这一政策的出台,有助于控制市场风险,保护投资者利益,维护金融稳定。在严监管下,代币交易平台被清理关闭。利用数字货币开展金融诈骗给社会带来的危害是巨大的,货币当局、金融监管部门及时出台政策,采取行动是非常必要的。

当然,中国人民银行对区块链技术的应用价值以及主权加密数字货币还是予以肯定,2015年1月,中国人民银行召开数字货币研讨会,对数字货币发行和业务运行框架、数字货币的关键技术等进行了深入研究。2016年2月,中国人民银行行长周小川在谈到数字货币相关问题时曾提及,区块链技术是一项可选的技术。2016年10月18日,中华人民共和国工业和信息化部发布了《中国区块链技术和应用发展白皮书》,围绕扶持政策、技术攻关和平台建设、应用示范等方面提出了相关建议。探讨由央行发行主权加密数字货币,规范数字货币的应用,维护数字货币体系的稳定,是摆在货币当局面前的重要课题。

四、结论与展望

通过对数字货币理论与实践进展的研究进行梳理,我们得出以下结论:首先,数字货币的出现是技术进步推动下的产物,中央银行发行主权数字货币可能代表未来数字时代的货币发展方向。从现代科技发展阶段来看,创新来自私人部门,私人数字货币先行发展,央行数字货币凭借主权优势迅速成为数字货币的主流形式是数字货币演进的基本路径。其次,数字货币的发展不是一蹴而就的,理论与实践还在不断探索当中,技术支持与制度建设还处在螺旋式上升过程中。央行数字货币还将面临来自技术与规制层面的各种挑战。第三,数字货币是伴随着信息技术的发展而产生与发展的,是由应用实践驱动的,数字货币的发展与支付环境密切相关,而支付技术的不断进步也会为数字货币形态的演进与创新提供更广阔的空间。再次,数字货币的规制建设与监管至关重要。需要对私人数字货币的定位、监管和准入制定权威标准,必须把私人数字货币纳入货币监管框架,与主权货币的边界区别清楚,其使用范围需要限定在局部范围之内。最后,数字货币的使用必然会对现代货币金融体系产生深远影响。在社会流通中表现为货币结构会多元化,央行数字货币价值相对稳定,而私人数字货币由于不具有主权信用而价值波动频繁,且货币领域的套利问题有可能引起市场波动。另外,货币运行机制会出现新的架构,传统的货币政策传导机制将会失效,重构货币政策体系与国家之间政策协调机制成为摆在各国央行面前的新课题。在国际货币体系中,超主权数字货币能否实现也取决于数字货币理论创新和各国数字货币实践政策的共同支撑,更需要国际组织的积极协调推进,构建相应的制度框架。

对于未来数字货币理论研究与实践发展的方向,本文认为主要集中在以下四个方面。

1. 数字货币的技术创新与研究。区块链技术是构造数字货币的基础技术,从比特币的区块链到以太坊、超级账本^④,区块链的技术还处于不断发展和完善的过程中,需要根据央行数字货币的实

际需求,研究一种适合中国的数字货币技术理论和构造方法。其中包括账本的格式、账本的内容、账本的溯源机制、账本的查询机制、账本的验证机制、账本的索引机制、账本的 Merkle 树^⑤验证机制等等。此外,还需要研究新的算法,解决系统效率及可扩展性问题等。

2. 数字货币的发行、存储、交易、结算理论的研究。在数字货币发行理论方面,根据数字货币的特点,在现有货币发行理论的基础上,借鉴国际数字货币实践经验,研究符合中国国情的数字货币发行理论,重点解决数字货币的需求、发行数量、发行方式、发行时间等一系列基础性理论命题。在数字货币存储理论方面,数字货币以分布式账本形式存储在区块链中,需要研究数字货币在商业银行账本的存储理论,以及在中央银行的区块链中存储的理论。商业银行存储部分的区块,会形成一个局部的区块链,中央银行将存储所有的数字货币交易的记录,并形成最终的区块链。需要重点研究数字货币在商业银行局部区块链的存储格式、存储位置、存储方法,在中央银行全球区块链的存储格式、存储位置、存储方法等。在数字货币交易理论方面,需要研究数字货币交易双方真实性验证、交易信息记账方法、交易信息账本确认方法、交易前的准备、交易中的处理机制、交易后的处理方法等等理论问题。在数字货币清算结算理论方面,需要研究数字货币的清算机制、模式与技术问题,可以借鉴 CBDC(Central Bank Issued Digital Currency)北航链的 ABC 和 TBC^⑥的清算与结算理论,进行相应的清算机制设计。

3. 数字货币的安全与隐私保护机制。当前,在数字货币应用中,普遍存在分布式账本中交易数据的保密问题、隐私与特权机制问题、计算和存储效率问题等。其中,运行安全风险、隐私泄露风险是数字货币安全的基础。因此,需要研究构建新型电子货币安全账本模型,研究分布式数字货币账本密钥泄露追踪和撤销技术,研究电子货币账本的隐私和匿名性等,以建立保证数字货币的安全与隐私的机制。

4. 数字货币的监管理论。由于数字货币的特殊性,需要重点研究数字货币在监管上的基础理论和技术应用,主要包括:研究数字货币监管模型、数字货币利率实施理论、数字货币 KYC(Know Your Customer)用户识别理论、数字货币反洗钱 AML(Anti-money Laundering)监管理论、数字货币大数据分析决策模型、数字货币“链上代码”^⑦执行理论等。通过研究数字货币的监管理论,实现中央银行对国民经济的宏观调控和各项货币政策的具体实施。

综上所述,数字货币理论研究与实践还在不断创新与探索之中,现代科技进步推动了数字货币形式的创新,中央银行主权数字货币代表未来数字货币的方向,与之对应的货币机制、货币理论与政策框架、货币规制与监管模式、国际协同模式等都需要在实践中不断完善。

注:

①资料来源: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>。

②资料来源: http://www.gov.cn/gzdt/2013-12/05/content_2542751.htm。

③资料来源: <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html>。

④超级账本(Hyperledger)是 Linux 基金会于 2015 年发起的推进区块链数字技术和交易验证的开源项目。

⑤Merkle 树,通常也被称作 Hash Tree,顾名思义,就是存储 hash 值的一棵树。

⑥ABC 和 TBC 是北航链中的交易链和账目链的简称,北航链是北京航空航天大学与北京大学联合开发的许可链,其设计初衷是为了公信和金融服务。

⑦链上代码是对智能合约的一种更为形象的表达。

参考文献:

贝多广 罗煜,2013:《补充性货币的理论、最新发展及对法定货币的挑战》,《经济学动态》第 9 期。

本·布劳德本特,2016:《中央银行与数字货币》,《中国金融》第 8 期。

范一飞,2016:《中国法定数字货币的理论依据和架构选择》,《中国金融》第 17 期。

贾丽平,2009:《网络虚拟货币对货币供求的影响及效应分析》,《国际金融研究》第 8 期。

贾丽平,2013:《比特币的理论、实践与影响》,《国际金融研究》第 12 期。

李志杰,2017:《法定与非法定数字货币的界定与发展前景》,《清华金融评论》第 4 期。

刘澜飏 沈鑫 郭步超,2013:《互联网金融发展及其对传统金融模式的影响探讨》,《经济学动态》第 8 期。

- 盛松成 蒋一乐,2016:《央行数字货币才是真正货币》,《中国金融》第14期。
- 万晨,2016:《数字货币国际监管动态及启示》,《金融时报》,2016年08月15日理论前沿版。
- 王永利,2016:《央行数字货币的意义》,《中国金融》第8期。
- 温信祥 张蓓,2016:《数字货币对货币政策的影响》,《中国金融》第17期。
- 徐忠 汤莹玮 林雪,2016:《央行数字货币理论探讨》,《中国金融》第17期。
- 谢平 刘海二,2013:《ICT、移动支付与电子货币》,《金融研究》第10期。
- 姚前,2016:《中国版数字货币设计考量》,《中国金融》第12期。
- 周光友 施怡波,2015:《互联网金融发展、电子货币替代与预防性货币需求》,《金融研究》第5期。
- 张正鑫 赵岳,2016:《央行探索法定数字货币的国际经验》,《中国金融》第17期。
- Ali, R. et al(2014), “Innovations in payment technologies and the emergence of digital currencies”, *Bank of England Quarterly Bulletin* 2014 (Q3):262-275.
- Ali, R. et al (2014), “The economics of digital currencies”, *Bank of England Quarterly Bulletin* 2014(Q3):276-286.
- Alstynne, M. V. (2014), “Why bitcoin has value”, *Communications of the ACM* 57(5):30-32.
- Back, A. (2002), “Hashcash—A denial of service counter-measure”, USENIX Technical Conference.
- Barrdear, J. & M. Kumhof(2016), “The macroeconomics of central bank issued digital currencies”, Bank of England, Staff Working Paper, No. 605.
- Bartos, J. (2015), “Does bitcoin follow the hypothesis of efficient market?”, *International Journal of Economic Sciences* 4(2):10-23.
- Bissessar, S. (2016), “Opportunities and risks associated with the advent of digital currency in the Caribbean”, Studies and Perspectives—ECLAC Subregional Headquarters for the Caribbean, No. 46.
- Bouoiyour, J. et al(2014), “Is bitcoin business income or speculative bubble? Unconditional vs. conditional frequency domain analysis”, MPRA Paper No. 59595.
- Bouri, E. et al(2016), “Modelling long memory volatility in the bitcoin market: Evidence of persistence and structural breaks”, Department of Economics, University of Pretoria, Working Paper Series, No. 54.
- Brown, W. L. (2014), “An analysis of bitcoin market efficiency through measures of short-horizon return predictability and market liquidity”, Claremont McKenna College Senior Theses, Paper 864.
- Chaum, D. (1983), “Blind signatures for untraceable payments”, in: *Advances in Cryptology: Proceedings of Crypto*, Springer.
- Chowdhury, A. & B. K. Mendelson(2014), “Digital currency and financial system: The case of bitcoin”, *Journal of Soils & Sediments* 6(4):268-268.
- Chuen, D. L. K. et al(2017), “Cryptocurrency: A new investment opportunity?”, <https://ssrn.com/abstract=2994097>.
- Conley, J. P. (2017), “Blockchain and the economics of crypto-tokens and initial coin offerings”, Vanderbilt University, Department of Economics Working Papers, VUECON-17-00008.
- Cretarola, A. & G. Figà-Talamanca (2017), “A confidence-based model for asset and derivative prices in the bitcoin market”, arXiv:1702.00215v1.
- Dai, W. (1998), “B-Money”, <http://www.weidai.com/bmoney.txt>.
- Donier, J. & J. P. Bouchaud(2015), “Why do markets crash? Bitcoin data offers unprecedented insights”, *Plos One* 10(10).
- Dwyer, G. P. (2015), “The economics of bitcoin and similar private digital currencies”, *Journal of Financial Stability* 17:81-91.
- European Central Bank (2012), “Virtual currency schemes”, <http://www.ecb.europa.eu>.
- Fernández-Villaverde, J. & D. R. Sanches(2016), “Can currency competition work?”, NBER Working Paper No. 22157.
- Frankel, A. S. (1998), “Monopoly and competition in the supply and exchange of money”, *Antitrust Law Journal* 66(2):313-361.
- Glass, J. E. (2016), “What is a digital currency”, *Journal of the Franklin Pierce Center for Intellectual Property* 57(3):455-517.

- Grinberg, R. (2011), "Bitcoin: An innovative alternative digital currency", *Hastings Science & Technology Law Journal* 4(1):160—207.
- Hanley, B. P. (2013), "The false premises and promises of bitcoin", arXiv:1312.2048v7.
- Nakaso, H. (2017), "Future of central bank payment and settlement systems under economic globalization and technological innovation", Bank of Japan, Remarks at the Forum Towards Making Effective Use of the BOJ-NET.
- Haldane, A. (2015), "How low can you go?", Speech given at the Portadown Chamber of Commerce, Northern Ireland, <http://www.bankofengland.co.uk>.
- Katsiampa, P. (2017), "Volatility estimation for bitcoin: A comparison of GARCH models", *Economics Letters* 158:3—6.
- Kurihara, Y. & A. Fukushima(2017), "The market efficiency of bitcoin: A weekly anomaly perspective", *Journal of Applied Finance & Banking* 7(3):57—64.
- Kraus, P. (2017), "Digital currency: Risks, rewards and investigative techniques", Doctoral Dissertation, Utica College.
- Koning, J. P. (2014), "Fedcoin", <http://jpkoning.blogspot.com/2014/10/fedcoin.html>.
- Mullan, P. C. (2014), *The Digital Currency Challenge: Shaping Online Payment Systems through US Financial Regulations*, Palgrave Pivot.
- Nadarajah, S. & J. Chu(2017), "On the inefficiency of bitcoin", *Economics Letters* 150:6—9.
- Nakamoto, S. (2008), "Bitcoin: A peer-to-peer electronic cash system", <http://bitcoin.org/bitcoin.pdf>.
- Ortisi, M. (2016), "Bitcoin market volatility analysis using grand canonical minority game", *Ledger* 1:111—118.
- Raskin, M. & D. Yermack(2016), "Digital currencies, decentralized ledgers, and the future of central banking", NBER Working Paper No. 22238.
- Szabo, N. (1998), "Secure property titles with owner authority", <http://nakamotoinstitute.org>.
- Swan, M. (2015), *Blockchain: Blueprint for a New Economy*, O'Reilly Media Inc.
- Šurda, P. (2012), "Economics of bitcoin: Is bitcoin an alternative to at currencies and gold?", WU Vienna University of Economics and Business, <http://nakamotoinstitute.org>.
- Shoaib, M. et al(2013), "Official digital currency", 8th International Conference on Digital Information Management (ICDIM), <http://ieeexplore.ieee.org>.
- The Financial Action Task Force (FATF) (2014), "Virtual currencies: Key definitions and potential AML/CFT risks", <http://www.fatf-gafi.org>.
- Urquhart, A. (2016), "The inefficiency of bitcoin", *Economics Letters* 148:80—82.
- Wallace, B. (2011), "The rise and fall of bitcoin", *Wired Magazine*, <http://laapush.org>.
- Woo, D. et al(2013), "Bitcoin: A first assessment", FX and Rates Research Report from Merrill Lynch, <http://www.w-t-w.org>.
- Wagner, A. (2014), "Digital vs. virtual currencies", *Bitcoin Magazine*, <https://bitcoinmagazine.com>.
- Yermack, D. (2013), "Is bitcoin a real currency? An economic appraisal", NBER Working Paper No. 19747.
- Zhu, Y. et al(2017), "Analysis on the influence factors of bitcoin's price based on VEC model", *Financial Innovation* 3(Article 3):1—13.

(责任编辑:刘新波)

(校对:李仁贵)