数字货币的源起、技术演进及未来趋势*

王 拓 刘晓星

（东南大学经济管理学院，江苏 南京 211189）

[摘 要] 随着区块链等科学技术的快速发展，数字货币逐渐成为全球竞争新的制高点。文章基于数字货币的诞生背景，对私人数字货币和法定数字货币的源起进行了阐述，从实物货币、信用货币与数字货币三个方面对货币发展的技术演进过程进行探讨，并通过回溯已有数字货币相关研究，从技术、监管及商业应用三个角度对数字货币的未来趋势开展深入研究。研究发现：比特币的出现对数字货币的发展具有标志性意义，法定货币系统因私人数字货币的盛行而受到一定程度冲击，当前英国、法国、加拿大、俄罗斯、中国等诸多国家均已开始进行法定数字货币研究或已将推出法定数字货币列入国家计划；数字货币主要包含共识机制、密码学原理、数据存储结构三大核心机制；当前数字货币在技术方面存在交易性能偏低、安全性隐患、隐私泄露等问题，未来可通过分链或跨链、改进加密算法等方式予以解决；在监管方面存在全球监管规则不统一、监管体系不健全、监管政策较片面等问题，未来法定数字货币的研究或推出将促进配套法律、制度等的变革发展，监管体系的不断完善将会对数字货币的发展方向起着决定性作用；在商业应用方面存在认可度低、应用范围较小等问题，未来随着法定数字货币及配套支付清算体系的推出，数字货币将在金融、全球贸易等领域发挥巨大的商业价值。

[关键词] 数字货币 数字货币源起 数字货币技术演进 数字货币未来趋势

[中图分类号] F821 **[文献标识码]** A **[文章编号]** 2096-983X（2021）05-0025-10

从远古时代的商品货币，到奴隶社会的金属货币，再到当前世界各国的纸币和电子货币，货币已历经了5000多年的发展。随着科学技术的快速发展，区块链、云计算、移动互联等新技术的推出，主权银行发行的传统信用货币迎来了新的挑战。随着区块链技术的出现，以比特币为代表的数字货币，使得每一个人都是货币的发行者，给法定货币系统带来了极大的冲击，数字货币可能成为未来货币发行、支付模式的发展方向，并逐渐成为全球竞争的新制高点。

一、数字货币的源起

（一）数字货币的诞生背景

著名的货币大师米尔顿·弗里德曼[1]在1991年完成的专著《货币的祸害——货币史上不为人知的大事件》的自序中写道：“在远古时代，当人们发现为获得某种东西而出售产品或服务

收稿日期： 2020-12-26

***基金项目：** 国家自然科学基金资助面上项目 “大数据驱动的金融风险管理与监控研究”（71673043）

作者简介： 王拓，博士研究生，主要从事金融科技、金融工程与风险管理研究；刘晓星，教授，金融学博士后，主要从事金融科技、金融工程与风险管理研究。

显得更为安全的时候，觉得很有必要把买与卖两种行为从单一的易货交易中分离出来——而这种东西并不会在生产中被消耗掉或用于生产，相反只是作为媒介，用来购买在生产中被消耗的或用于生产的产品或服务。连接买与卖两种行为的‘某种东西’被称作货币，其千百年来以各种不同的物理形式出现——从石头、羽毛、烟叶、贝壳，到铜、白银、黄金，甚至到现在的纸币和分类账簿中记录的条目。谁知道未来的货币会演化成何种形式？会是计算机字节吗？”

未来总比预测来得要快。在弗里德曼提出猜想不到20年时间里，在云计算、互联网、移动互联网、智能化、大数据等现代科学技术迅猛发展的基础上，几乎所有经济金融活动都被搬到了互联网上，尤其是移动互联网上。互联网让世界变成了地球村，移动互联网让世界变成了“手掌心”，数字货币自然也将是手掌心交易不可或缺的价值交换工具。

任何一种货币的诞生和发展，都有其独特的历史背景。数字货币的诞生也并非独立事件，其源起于美元脱离金本位。二战结束后，美国成为了世界秩序的主宰。在金融秩序方面，美国建立了布雷顿森林体系，即美元与黄金挂钩，指定美元为世界各国的支付手段，形成了以美元为中心的世界货币体系。然而黄金产量有限，随着社会经济及金融的不断发展，美联储的黄金储备无法衡量布雷顿森林体系系统里美元的价值。1971年美国总统尼克松时代美联储废除了金本位，美元不再锚定黄金，取而代之的是以美国信用背书的主权货币。这一变化引发了全球经济学家的不安，这意味着美国可以自由增发货币来掠夺财富，事实证明确实如此。津巴布韦的货币贬值即为典型案例，40万亿津元兑换1元人民币，价值还不如我国冥币。1976年奥地利经济学家哈耶克提出“自由市场经济学”理论，提出私人银行发行可竞争货币的概念，这便是“数字货币”（包括当今比特币）的雏形。而同年Diffie（Sun公司前首席安全官）和Hellman（斯坦福大学教授）[2]发明了Diffie-Hellman算法，首次提出了非对称加密体系，为当今数字货币的发展奠定了重要基石。

1982年，大卫·乔姆[3-4]首次提出了数字货币理论，其基于传统的“银行—个人—商家”模式提出的电子货币系统，具备不可追溯、匿名性等特点。虽然该电子货币系统未能成功，但大卫·乔姆提出的数字货币理论激发了研究者对数字货币的广泛兴趣，且其提出的两项关键技术——随机配序和盲签名一直沿用至今。

1996年由著名肿瘤学家Douglas Jackson发起的E-Gold数字货币，是第一个以黄金为支持的数字货币，其活跃用户一度达到500万，后来平台持续遭遇黑客攻击并吸引了大量非法洗钱交易，使该数字货币遭遇各国政府封杀。

WebMoney是一家总部位于莫斯科的公司，它提供广泛的点对点付款解决方案，涵盖互联网交易平台。该公司于1998年推出的WebMoney是一种通用数字货币，它也是少数幸存的未加密数字货币之一。时至今日，该货币仍被数百万人广泛使用和接受。与此同时，它也可以转换为法定货币，如卢布、美元、英镑甚至比特币。

中本聪[5]于2008年在《比特币：一种P2P的电子现金系统》一文中首次提出比特币的概念，指出比特币是基于P2P网络的一种去中心化的电子现金系统，交易双方可以绕开央行等第三方机构，通过比特币直接完成转账交易。比特币采用区块链技术，将交易信息存储在分布式账本中，具备去中心化、总量有限、交易安全、信息公开的超时代的特点。比特币的出现标志着一个新的数字货币时代诞生，比特币的普及推动着数百上千种加密货币的研究与发明。

（二）私人数字货币的发展

数字货币以数学理论为基础，运用密码学原理来实现货币的特性。数字货币主要采用对称性密码算法、非对称性密码算法、哈希函数等加密算法，常用的技术有数字签名、零知识证明和盲签名技术等[6]。

根据不同的分类标准，数字货币可以分为不同类型。若以发行主体为分类依据，数字货币

可以分为法定数字货币与私人数字货币两类[7]。目前，最具代表性的私人数字货币主要是比特币。比特币的核心特点即为去中心化，其以区块链作为底层技术，借助分布式共识、加密数据、P2P算法、时间戳等方式，通过分布式网络帮助用户完成点对点交易，为目前银行等中心化机构常见的效率低、交易成本高等问题提供了新的解决思路[8]。

根据是否采用分布式记账技术，数字货币则包括加密数字货币与非加密数字货币两类。加密数字货币最典型的特点是采用了分布式记账技术，比特币是史上第一个加密数字货币。以太币对比特币的可编程脚本技术进行延伸，目前已发展为世界第二大数字货币，其工作机制不同于比特币，前期采用POW机制挖矿，后期将转为POS（Proof Of Security，股权证明）机制；达世币设置了双层奖励制网络，其主要特点是支付的即时性和匿名性，支付即时性达到秒级，其匿名性则接近于在生活中使用现金；门罗币吸收比特币社区发展出的机密交易技术隐藏交易金额，并运用环签名技术隐藏交易双方地址，提供了更完善的匿名性；零币首次将零知识证明算法zk-SNARK用于保证交易发送者、接收者和交易数额的隐私性，具有较强的学术创新。加密数字货币中较为知名的还有莱特币（Litecoin）、狗狗币（Dogecoin）、点点币（Percoin）等 。非加密数字货币即未采用分布式记账技术的数字货币，瑞波币（Ripple）即是典型的非加密数字货币[8]。瑞波币是一个开放支付网络，允许不同的网关发行各自的借据（IOU，I Owe You，相当于在线债券的借据），并实现不同借据之间的自动转换；瑞波币不仅包括数字货币，还包括国家法币。

比特币出现后，去中心化的数字货币进入大规模试验阶段，基于不同区块链创新技术的各类数字货币层见叠出。截至2019年10月27日，出现的数字货币超过2千种，市值达到1.9万亿，比特币市值维持在1.2万亿，为目前全球市值最大的数字货币，占全球数字货币总市值的63.2%。以太坊和瑞波币以1412亿和912亿人民币成为全球市值第二、第三大数字货币。当前以比特币为代表的私人数字货币因其去中心化、交易安全、不易篡改等优点正在被广泛接纳，而正是其去中心化的特性成为私人数字货币替代信用货币的最大障碍，因其对当前各国货币的发行理念及机制提出了挑战，截至目前，私人数字货币的清偿、支付等功能仍未得到认可，其货币属性未被全球任一国家所承认[9]。私人数字货币没有国家信用背书，不具备货币职能，其本质是一种商品而非货币。

（三）法定数字货币的发展

作为科技创新与金融创新相结合的产物，数字货币的出现及发展与当前货币体系存在的缺陷密不可分[10]。尽管加密数字货币所引起的“三反”（反洗钱、反恐怖融资、反逃税监管）及资本外流问题令各国政府头疼，但其跨区域、匿名性、低成本、高效率等超时代的优良特性，在提升效率、降低支付成本、保护用户隐私等方面带来的积极影响不容忽视。在此背景下，各国央行开始积极探索数字货币背后的技术对本国货币体系的借鉴之处，法定数字货币的春风在世界各地吹起。

最先试水法定数字货币的是南美洲国家厄瓜多尔，2015年2月厄瓜多尔推出了一种“电子货币系统”和基于这个系统的“厄瓜多尔币”，通过资格认证的市民可以通过移动App利用厄瓜多尔币在超市、商场、银行等场所完成支付以及转账等操作。然而，厄瓜多尔币并未像预期一样普及开来，并于2018年3月底宣告停止运行，草草收场。委内瑞拉政府则于2018年2月21日发行了官方数字加密货币，即“石油币”，成为南美洲第二个推出央行数字货币的国家。石油币被寄予拯救委内瑞拉全国于经济泥潭的希望。石油币发行规模为1亿个代币，总价值超过60亿美元，石油币发售首日就完成了7.35亿美元的融资。但自去年2月发行以来，石油币的交易量仅仅300多个，与其1亿总发行量相比不值一提。在国际层面，石油币也遭到美国方

面全面打压，特朗普签署行政令，全面禁止“石油币”在美流通，石油币的未来堪忧，难破重围。同为2018年2月，大洋洲国家马绍尔群岛通过立法正式宣布将发行新的国家数字货币—“Sovereign”，与美元一同在国内流通。此外，乌拉圭、突尼斯及塞内加尔也都发行了各自国家的央行数字货币。从已发行数字货币的国家来看，要么国际上经济地位不高，要么是国内面临严峻的经济困境，急寻出路。事实上，最后也并未取得预想中的效果，未能在全国范围内得到采用。

与上述国家急于推出数字货币寻求出路不同的是，作为世界经济大国的美国和日本，目前均没有推出央行数字货币的计划。中国、俄罗斯、瑞典、泰国、立陶宛、巴哈马等国家，已将推出法定数字货币列入计划。而支付体系长期由美国三大巨头（PayPal、VISA、MasterCard）主导的欧洲诸国，在Facebook发布Libra白皮书后加快了对央行数字货币的研究工作。早在2016年，英国中央银行便推出了其法定数字货币框架—RSCoin，旨在强化英国经济和全球贸易，该货币结合了新分布式账本技术的优势和传统中心化的管理货币形式，是一种“混血”货币。2019年9月17日，欧洲央行管委维勒鲁瓦对外透露，法国央行已经开始研究央行数字货币。而与英国、法国一样，加拿大、新加坡、巴西、丹麦、挪威、以色列、菲律宾、以色列等诸多国家也早已紧锣密鼓地展开了对央行数字货币的研究。

中国人民银行是最先开始对数字货币展开实验与研究的中央银行，早在去中心化数字货币尚未成为风潮时，我国央行就已探索这一领域[11]。2014年，在时任行长周小川的带领下，央行便成立了专门的加密货币研究小组，负责制定数字货币DC/EP发行与操作的框架，正式启动了法定数字货币研究。2015年央行持续充实力量，对货币演进中的数字货币、数字货币发行的总体架构、央行发行的加密数字货币等九大专题展开研究。2016年我国组建了央行数字货币研究所，专门承担法定数字货币研发工作，争取早日推出央行数字货币。2017年，研发工作进入新的阶段。经国务院批准，中国人民银行组织相关市场机构开展名为DC/EP（Digital Currency/Electronic Payment）的法定数字货币分布式研发工作。2018年，中国人民银行以数字货币研究所作为出资方，正式组建从事数字货币等金融科技领域研究的金融子公司——深圳金融科技有限公司，为央行数字货币落地奠定基础。2019年8月10日，中国人民银行支付结算司副司长穆长春在“第三届中国金融四十人伊春论坛”上透露央行数字货币原型已研制成功，指出我国央行数字货币将运用“双层运营体系”，即数字货币先由中国人民银行向银行或其他金融机构等进行兑换，上述机构再将数字货币兑换给民众。2019年10月28日，黄奇帆以中国国际经济交流中心副理事长的身份在首届外滩金融峰会上亮相，指出央行数字货币的意义在于它不是现有货币的数字化，而是M0的替代。央行数字货币有利于减少交易环节对账户的依赖，促进人民币的流通与国际化[12]。我国央行数字货币呼之欲出，其成功发行对我国乃至世界货币体系都具有里程碑意义。

除了各国进行法定数字货币的研发，跨国机构也开始布局数字货币。先有摩根大通推出“JPMCoin”后有脸书发行Libra白皮书，再有沃尔玛申请数字货币领域专利。总体而言，自比特币出现的十年来，底层技术区块链一度被神话，比特币投资价值受无数投资者疯狂追捧，但随着时间的推移，市场情绪渐趋冷静，数字货币行业从最初的无序发展正转向繁荣。当前，数字货币和区块链的正向价值开始被各国和众多技术公司所重视，随着国家和全球知名企业的入局，数字货币的发展正进入一个全新的时代。

二、数字货币的技术演进

货币的演进往往伴随着技术的发展。商品货币向金属货币演进是冶金技术的进步，金属

货币向纸币演进是印刷技术的进步，而纸币向电子货币演进则伴随着计算机及互联网技术的进步。货币发展到现在其信用货币的本质已经基本成型，但货币的具体表现形式还会随着技术的进步不断演化、发展[13]。1948年12月我国第一套人民币发行，随着材料、印刷技术、防伪技术等的进步与发展，我国人民币至今已更新至第六套。而20世纪90年代互联网的普及，网络经济和电子商务兴起，推动了货币的电子化。随着互联网金融的快速发展，从1993年我国首次建设电子支付系统至今，第三方支付和移动支付系统已全面普及。目前，由于区块链技术的出现与应用，货币正从电子货币形式向数字货币形式转变。自2008年比特币诞生以来，全球数字货币的发展过程积累了很多技术成果和经验，如优化的共识算法、更加合理的分布式存储技术、更加安全的加密算法、更加合理的区块链账本格式和内容等，这些都对数字货币的技术演进与创新具有显著意义。

（一）数字货币的核心技术概述

数字货币是多种技术结合的产物，其主要基于节点网络和数字加密算法，呈现出去中心化和不可篡改的核心性质。当前以比特币为代表的主流数字货币均以区块链技术为底层支撑技术。区块链是由节点参与的分布式数据库系统，其主要包含共识机制、密码学原理、数据存储结构三大核心机制[14-15]。

1. 共识机制

共识机制是区块链技术的核心组件。区块链解决了在不可信信道上传输可信信息、价值转移的问题，而共识机制解决了区块链如何在分布式场景下达成一致性的问题。共识机制就像是区块链国家的法律，维系着区块链正常、稳定地运转。截至目前，主要的共识机制包括工作量证明机制（POW）、股权证明机制（POS）、拜占庭一致性协议机制（PBFT）等[14]。

POW的核心理念是按劳分配，即谁的工作量大、谁的收益就越大。POW最常见的应用便是比特币，在该机制网络中，节点通过计算随机哈希散列的数值解来争取记账权，谁优先得出正确的数值解，谁的算力就越大，谁记账的概率也就越大。POW具有完全去中心化的特点，在以该机制为共识的区块链网络中，节点可以自由进出，当前比特币网络就利用该机制产生新的数字货币。但与此同时，该共识机制对节点的网络性能要求高，资源浪费严重，达成共识所需周期较长，效率低下，因此该机制不适合广泛商业应用。

POS的核心思想是持有更多币（包括持币时间）的矿工将获得更多的投票权。相较于POW，POS最大的优点是可以大大缩短达成共识的周期，减少资源浪费，但在以POS为共识的区块链网络中，几乎仅有拥有一定数量加密货币所有权的节点才有机会取得记账权，资源相对缺乏的节点则很难拥有记账权的机会，不能达到完全去中心化。POS最早在Peercoin系统中被实现。

区块链的去中心化程度主要取决于选用何种共识机制。选用的共识机制不同，区块链的去中心化程度往往有所差异，其处理效率、资源耗费等性能也会受到影响。一般而言，区块链的效率等性能与其去中心化程度呈现反向关系，即区块链的去中心化程度越高，往往意味着处理效率越低。

2. 密码学原理

区块链技术应用的密码学原理之一为非对称加密技术。非对称加密又称公开密钥加密，是一种密码学算法类型，该加密算法使用公开密钥和私有密钥两个不同的密钥。区块链网络中，任一节点都有且仅有一对公开密钥和私有密钥，如若用公钥对数据进行加密，只有用对应的私钥才能解密。在区块链网络中，私有密钥是控制权的体现。交易一方可以使用自己的私钥对交易信息进行签名后再连同对应的公钥一并公开，交易对手方收到消息后再用交易发起方公开的密钥对交易进行验签。非对称加密技术消除了最终用户交换密钥的需要，交易发起者不需要向交易对手方传输自己的私钥即可完成

交易，保密性较好。

区块链技术应用的密码学原理之二为哈希算法。哈希算法是一个密码散列函数，也称为散列，可以把任意大小和长度的输入，通过散列算法变换成固定大小和长度的输出，而根据哈希算法输出的信息进行逆向推算几乎不可能。浅显来说，哈希算法的输出值就像是一篇文章的摘要，从整篇文章概括出摘要比较简单，但若根据摘要将文章还原则几乎不可能发生（哈希函数的隐秘性）。哈希算法是区块链系统安全的重要保障技术之一，因其加密或验证简单、信息敏感性（加密信息细微的改变便会导致输出值发生根本变化）等特性广泛应用于数字货币中。

3. 数据存储结构

默克尔树（Merkle Tree）本质是一种储存哈希值的树状数据结构，通常也被称作哈希树（Hash Tree），由数据块、叶子节点、中间节点和根节点组成。Merkle Tree广泛应用于比特币网络中，以一种非常有效的节省空间和时间的方式，来帮助验证交易的存在。Merkle Tree可用于归纳一个比特币区块中的全部交易，每笔交易对底部数据块进行哈希运算得出的哈希值为叶子节点，再对相邻的两个叶子节点进行哈希运算得到的哈希值生成中间节点，最终得到所有交易的哈希值即为根节点。如果篡改任意一笔交易，最终得到的默克尔树根就完全不同，因此通过验证Merkle Tree的根哈希即可达到验证交易的目的。

（二）数字货币的技术演进

1976年，迪菲（Diffie）和赫尔曼（Hellman）[2]在一篇题为《密码学的新方向》的论文中提出了一种完全不同于对称密码体系的新思路，构造出一种加密密钥与解密密钥不一样的非对称密码体系；1978年麻省理工学院（MIT）的李维斯特（Rivest）、萨莫尔（Shamir）等[16]在《获得数字签名和公钥密码系统的方法》论文中[5]，构造了基于因子分解难度的签名机制和公钥加密机制，首次提出非对称加密的实现算法：著名的RSA密码算法。非对称加密思想的提出以及1978年RSA算法的实现，开启了现代密码学新时代，对数字货币的技术实现具有里程碑意义。

数字货币系统起源于荷兰，最初由David Chaum于1982年在其《用于不可追踪的支付系统的盲签名》的研究中提出，这种命名为E-cash的数字货币系统是基于“个人-银行-商家”的三方交易模式。E-cash虽然未能取得成功，但其中用到的两项关键技术对当今数字货币系统的发展具有深远的意义。第一项技术是随机配序。随机配序产生唯一的序列号，从而确保了数字货币的唯一性，保证数字货币不会被重复使用。第二项技术是盲签名。该项技术是基于RSA算法的新密码协议，能够确保银行或数字货币发行机构对该数字货币的信用背书。

哈希算法的多样化与革新是数字货币技术演进过程中的另一关键阶段。哈希算法的初始标准之一是MD5哈希，该算法功能简单，不论输入何种信息，输出的都是一个固定的128位字符串，且其仅通过几轮单向运算来计算出确定性输出值，因此其很容易被破解并易受到“生日攻击”的侵扰。美国国家安全局（NSA）一直都是哈希算法标准方面的先驱，他们最早于1995年提出安全哈希算法，也就是SHA1，这个算法输出的是160位固定长度的字符串。然而，SHA1仅仅在MD5的基础上提高了输出的长度，单向操作的数量以及单向操作的复杂性并未做任何根本改进，因此其仍然无法抵御更强大的机器攻击。直到2006年，美国国家标准与技术研究所（NIST）通过竞赛的形式寻找到了与SHA2从根本上不同的替代品——SHA3，成为新的算法标准。SHA3又被称为KECCAK哈希算法，与之前的算法完全不同的是，SHA3内部拥有海绵结构（Sponge Construct）机制。这种结构使用随机的排列组合来吸收和输出数据，同时还能为未来输入值提供随机源。SHA3的诞生是哈希算法伟大机制的一部分，是数字货币技术演进的关键进程。

2008年11月1日，中本聪[5]在其发表的《比特币：一种P2P的电子现金系统》文章中提出了通过P2P技术完成交易的全新电子现金系统，用去中心化的P2P交易模式代替David Chaum的三方交易模式。区块链技术使得比特币实现了分布式共享账本，解决了E-cash数据库无限膨胀的问题，使数字货币技术出现质的飞跃[17]。

当前区块链已在各种各样的场景中被广泛应用，数字货币也已进入新的发展阶段，但在技术性能、安全性隐患等方面，区块链仍然面临较大挑战。区块链技术的核心特征之一便是分布式共享，因此其在交易性能、资源耗费等方面仍存在缺陷，当前比特币交易大约需要1小时才能完成。此外，数字货币交易系统黑客攻击事件频发，区块链仍存在较大安全隐患，如2016年发生的以太坊项目黑客攻击事件。区块链技术是对传统计算机与信息技术的更新和升级，未来发展应加强与5G、人工智能、大数据等其他新兴信息技术的融合，相互促进，优势互补，让区块链为央行数字货币的发行奠定坚实的基础。

三、数字货币的未来趋势

（一）数字货币未来趋势之技术

目前，全世界还没有一家央行推出真正意义上的法定数字货币，数字货币技术主要应用在私人数字货币领域。在私人数字货币运行的十多年中，虽然在技术上取得了一定的突破，但作为底层支撑技术的区块链仍处于起步发展阶段，在实际应用场景中仍存在交易性能偏低、交易安全性、隐私保护以及标准统一等主要问题。

1. 交易性能

以比特币为例，比特币网络目前能够承载的交易量在每秒7笔左右，这与目前交易系统需要的每秒十万笔以上的要求相去甚远。对于交易性能偏低的问题，也出现了一些解决方案方案[18]。例如闪电网络，用户由于对于小额交易来说交易效率或者交易速度的权重要显著高于交易安全性的权重。对于小额的交易，可以在比特币区块链外建立一个专门用于小额交易的资金池。由专门的节点来负责对资金池进行运营，在达到一定的金额或者一段固定的时间（比如一个月）再将交易的总金额添加到比特币区块链中。这样的交易机制设计能够提高比特币的支付效率。对交易的安全性则由可信节点来保障。第二种解决方案为分链，将比特币区块链分为主链和侧链，这样主链上的每一个节点都可以变成分链的创始节点，这样极大地扩充了区块链的容量。比特币的交易可以通过匹配算法选择处于空闲状态的侧链来创建交易。第三种技术解决方案为跨链技术。跨链是指在不同的两条或多条区块链之间建立起信息流通的机制。由于目前私人数字货币的迅猛发展，已经产生了多达数千种的数字货币。这些私人数字货币大多基于区块链技术，因此已经构建了很多的数字货币基础设施。跨链技术能够建立起不同区块链之间的有效沟通机制。因此等到市场竞争开始整合各种不同的私人数字货币时，跨链技术就能将这些数字货币的基础设施充分利用起来，减少区块链的重复建设，也因为跨链技术高效的链间沟通使得区块链网络的运行效率大幅度提高。

另外，考虑到5G技术已经开始投入商用，使得现有移动互联网的网络传输速度呈几十倍乃至一百倍的增长，区块链处理交易的速度也会有大幅度的提高。人工智能、大数据、物联网等新兴技术和区块链的结合还有广阔的创新空间。

2. 安全性隐患

安全问题自互联网产生就与之伴随在一起，进入移动互联网时代，安全更是成为摆在各大互联网公司之前的首要问题。不管是央行数字货币还是私人数字货币，由于是金融资产或者支付工具，因此对安全性有更高的要求。

自私人数字货币出现以来，已经发生了多起安全问题。2011年6月MT.Gox网站遭到黑客

攻击，造成近6万名用户的信息被泄露，黑客以管理员身份登录网站，大量发售比特币。结果造成比特币价格由17.51美元暴跌至0.01美元。2013年10月，美国FBI因毒品交易关闭Silk Road网站，并没收26000个比特币。2017年8月，全球最大的美元交易平台Bitfinex出现安全漏洞导致用户的119756个比特币被盗，总价值超过7500万美金。2017年11月，比特币交易平台Tether被黑客入侵，有价值超过3000万美金的比特币被盗。2017年12月，全球最大的数字货币挖矿平台NiceHash的支付系统被黑客入侵，有价值超过5000万美元的比特币被盗。

由此看出，私人数字货币交易平台安全事故频发，安全形势不容乐观。在传统的货币体系中，法定货币一般拥有专用的网络。专用网络使得交易的安全性得到了保障，但由于各个国家都有自己的专用网络，而且没有统一的、标准化的接口，因此交易的效率较低。特别是跨境转账、跨境支付不仅交易时间长而且交易费用高。私人数字货币出现的一个重要原因就是为了实现便捷的跨境支付。

解决安全隐患不仅仅是不断改进加密算法，更要从平台的管理机制设计上考虑。从已经发生的安全事故来看，数字货币本身是非常安全的，黑客很难篡改区块链上的数据。安全事故往往发生在数字货币的交易平台或者管理平台。因此集中力量建立安全的数字货币基础设施是十分必要的。

3. 隐私保护

私人数字货币从诞生之初就非常重视隐私保护，中本聪在设计比特币时，一个重要的设计理念就是要保护用户的匿名性。区块链的特点之一是透明、可追溯，但对比特币的使用者信息是匿名的。这一点也是许多用户使用比特币的重要原因。但目前大型互联网公司如Facebook、苹果等用户隐私泄露事件频发。在中国，很多用户信息被非法出售，用户经常接到各种骚扰电话，收到各种骚扰短信。如何设计有效的机制来激励私人数字货币发行机构保护用户隐私成为主要的问题。2019年6月，Facebook发布的Libra白皮书基础由非盈利机构来负责其发行的数字货币的运营。该机构由若干会员组成，各成员都仅有较小一部分投票权，因此不会为了某一会员的利益而破坏用户隐私保护。

（二）数字货币未来趋势之监管

当前数字货币的定义及货币属性尚未定论，世界各国对数字货币的监管政策及监管力度存在很大差异。根据coindance数字货币交易平台（https://coin.dance/poli）的统计显示，在全球251个国家中，未限制数字货币交易的国家达到111个。从目前的各国政府针对私人数字货币监管发布的文件来看，美国、日本、新加坡对私人数字货币还是抱着比较开放的态度，而中国、俄罗斯、欧盟对私人数字货币持相对谨慎的态度[19-20]。

1. 全球监管规则不统一

对于金融科技产物，美国方面一向都持比较开放的监管态度，早在2012年，美国国会就召开了比特币的听证会。2015年，纽约州率先通过全球第一个交易数字货币的执照Bit license。美国的州际统一法律委员会通过了《虚拟货币商业统一监管法》，对“数字虚拟货币”做出了明确定义，并对金融监管机构的监管要求提出了明确的规定[21]。

英国、瑞士等欧洲国家的监管态度与美国相似，强调中立原则，积极拥抱新兴科技产物，将包括私人数字货币在内的一切金融活动和机构纳入审慎监管体系，认为目前监管制度与体系照样适用于数字货币的监管。

相对于美国和欧洲，日本则采取了更进一步的监管措施。2016年，日本对《资金结算法》及配套法律法规进行修订，重新建立了金融监管架构。贺同宝[22]指出这些法律文件对加密货币的监管部门、监管规则及法律属性作出明确规定，把数字货币交易纳入监管体系，同时从立法维度搭建了适用数字货币的监管架构。

而中国、俄罗斯、泰国等国家则明确禁止了私人数字货币的发行与交易。中国早在2014

年便出台相关文件禁止一切比特币等加密货币的市场行为；俄罗斯政府也对比特币予以明令禁止，认为比特币的普及可能会一定程度上替代其法定货币；韩国政府于2017年9月，同样开始对一切形式的数字货币发行融资活动予以禁止，并于当年年底组建专门的数字货币对策小组对数字货币的过度投机行为进行监管。

当前数字货币监管尚未存在统一的监管规则，目前数个国家指出各国政府应加强协作，共同克服困难，迎接数字货币监管带来的挑战[23]。2018年，二十国集团在G20峰会上表示各国政府应提升国际协作意识，制定全球统一的数字货币监管规则；同时希望金融行动特别工作组（FATF）制定审查标准，加强全球监管意识，在FATF的审查标准体系下来管理数字货币。由于数字货币交易的全球性，制定全球统一的监管制度和审查标准将是必要之举。

2. 中国监管“一刀切”

针对私人数字货币，我国采取了非常严格的监管措施，央行等五部于2013年12月，下发《关于防范比特币风险的通知》，2014年3月央行发布《关于进一步加强比特币风险防范工作的通知》，严禁比特币作为流通货币使用，且对金融机构从事私人数字货币业务的行为予以禁止。中国人民银行于2017年9月又联合七部委发布了《关于防范代币发行融资风险的公告》，不但严禁各种代币发行融资活动，也严禁各金融平台及第三方支付机构从事与代币发行融资有关的业务。

针对法定数字货币，我国则采取积极推进的态度。央行早在2014年就开始法定数字货币研究工作，并于2016年组建了数字货币研究所，致力于发行由国家信用来背书的主权数字货币。这势必使得中国政府对私人数字货币实行严监管的政策。2019年10月25日习近平主席主持召开区块链集体学习的第二天，我国第十三届人大常委会第十四次会议表决通过了密码法，旨在规范密码应用和管理，保障网络与信息安全。密码法的颁布将提升对数字货币的法治化监管，为未来数字货币的发展创造更安全的环境。

林毅夫[24]指出，经济发展的过程也是基础配套、技术、制度、监管体系等不断变革发展的过程，不仅需要市场有效，同时也需要政府有为。私人数字货币是科技领域与金融领域结合创新的产物，各国的科技巨头和金融巨头均开始布局数字货币市场，如美国银行巨头摩根大通于2019年2月发布了旗下的私人数字货币产品摩根大通币，其直接代表美元，用于客户之间的即时结算；科技巨头Facebook于2019年6月18日正式上线全球加密数字货币Libra，其将区块链与比特币的优势相结合，对发行机制、支撑技术等进行升级改造，计划建立一套简单的、无国界的货币及为上10亿人所服务的金融基础设施。王靖一等认为若Libra的储备框架中引入一家或几家央行，通过“合成型CBDC”成功实施，则可能会撼动当前金融体系的基石，甚至对央行货币政策带来巨大冲击。因此面对私人数字货币，中国应拥抱创新与挑战，在鼓励中国央行推进法定数字货币研发的同时，也应鼓励中国企业与Libra等私人数字货币加强合作。中国不能因为私人数字货币乱象问题而对其进行全面否定，而应尽快将其纳入监管体系，并从立法层面搭建适用于私人数字货币的监管框架，规范私人数字货币市场，充分发挥私人数字货币创造商业价值的能力。

（三）数字货币未来趋势之商业应用

数字货币相比目前的纸币体系运行成本更低，而且远距离交易更加方便，因此数字货币未来可能广泛应用到跨境支付以及全球贸易中。

中国人民银行对于发行央行数字货币已经做了很长时间的研究，认为央行数字货币首先应该是取代目前交易中的现金部分，即M_0。央行数字货币若要提高市场占有率及用户使用率，则必须适应现金的使用场景。现金的使用一般具有高频率、低金额的特点，为了适应这些特点，央行数字货币支付清算体系必须高效快

捷。在中国发达的电商网络下，孕育了许多互联网公司推出的支付系统。央行数字货币作为以国家信誉背书的法定数字货币，如果能将众多的小额支付体系整合起来，对于提高整个社会的支付效率具有重大意义。

在完成对交易中现金的取代后，接下来就要代替银行中的电子货币。央行数字货币取代商业银行账户上的电子货币主要是基于安全上的考虑。目前商业银行的数据存储是中心化的，一旦遭遇网络攻击有可能蒙受巨大损失；而央行数字货币采用的是分布式存储方式，有多个节点保存了用户信息，某一个节点受到网络攻击并不会对整个数字货币系统产生大的影响。此外，由于央行数字货币采用的分布式存储方式有多个计算节点的存在，数字货币体系的计算能力也更强，支付清算系统效率则更高，而更快的支付清算能够降低汇率风险，提高资金周转率，这在国际贸易中将会起到重要的作用。在央行搭建好关于数字货币的大额和小额支付体系后，更多细分的支付需求就可以让支付宝、财富通等支付公司，基于不同需求进行平台升级或开发，通过数字货币在商业上的应用，使得支付变得更安全、更经济、更便捷。

参考文献：

[1]Milton Friedman. 货币的祸害[M]. 北京：商务印书馆，2006.

[2]Whitefield Diffie and Martin Hellman. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22（6）：644-654.

[3]David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24（2）：84-90.

[4]David Chaum. Blind signatures for untraceable payments, advances in cryptology[J]. In Proceedings of Crypto, 1982：199-203.

[5]S. Nakamoto. Bitcoin：A peer-to-peer electronic cash system[EB/OL].（2008-11-01）[2020-12-26]. https://library. uniteddiversity. coop/Money_and_Economics/bitcoin. pdf.

[6]姚前，汤莹玮. 关于央行法定数字货币的若干思考[J]. 金融研究，2017（7）：78-85.

[7]姜其林，苏晋绥，米丽星. 基于央行视角下我国法定数字货币发展趋势与监管挑战[J]. 华北金融，2020（4）：84-94.

[8]李建军，朱烨辰. 数字货币理论与实践研究进展[J]. 经济学动态，2017（10）：115-127.

[9]邱勋. 中国央行发行数字货币：路径、问题及其应对策略[J]. 西南金融，2017（3）：14-20.

[10]阎迪. 推进法定数字货币建设及政策建议[J]. 当代经济，2018（7）：56-57.

[11]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.

[12]蒋鸥翔，张磊磊，刘德政. 比特币、Libra、央行数字货币综述[J]. 金融科技时代，2020（2）：57-68.

[13]郭庠林. 中国古代的货币管理[J]. 财经研究，1987（7）：48-51；61.

[14]连一席. 区块链研究报告：从信任机器到产业浪潮还有多远[J]. 发展研究，2018（8）：16-29.

[15]谢开斌. 基于区块链的数字货币演化[J]. 计算机应用研究，2019，36（7）：1935-1939.

[16]R L Rivest,A. Shamir L. Adleman. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 26（2）：96-99

[17]姚前. 数字货币的前世与今生[J]. 中国法律评论，2018（6）：169-176.

[18]王思轩. 区块链技术对支付结算的挑战与对策——以“技术治理”为视角[J]. 现代经济探讨，2020（1）：93-100.

[19]华秀萍，夏舟波，周杰. 如何破解对数字虚拟货币监管的难题[J]. 金融监管研究，2019（11）：1-18.

[20]李文红，蒋则沈. 分布式账户、区块链和数字货币的发展与监管研究[J]. 金融监管研究，2018（6）：1-12.

[21]柯达. 数字货币监管路径的反思与重构——从“货币的法律”到“作为法律的货币”[J]. 商业研究，2019（7）：133-142.

[22]贺同宝. 国际虚拟货币监管实践研究[J]. 北京金融评论，2018（3）：3-7.

[23]佘茂艳，王元地. 数字货币发展现状及其监管[J]. 中国矿业大学学报（社会科学版），2020，22（2）：121-130.

[24]林毅夫. 产业政策与我国经济的发展:新结构经济学的视角[J]. 复旦学报（社会科学版），2017，59（2）：148-153.

【责任编辑　许鲁光】

（下转第108页）