微信扫码看作者独家介绍本论文

区块链技术国外研究述评

韩秋明[1,2] 王 革[1]

(1.中国科学技术发展战略研究院,北京 100038;2.南开大学 经济与社会发展研究院,天津 300071)

摘 要:区块链技术为多种服务提供了一种新型信任机制,具有很强的催化效应,可能对多种社会服务带来颠覆性影响。基于国际组织和各国政府对区块链技术的预判与实践,分析 Web of Science 中有关区块链技术的研究论文。研究认为,目前区块链技术研究主要聚焦在隐私保护、智能合约、资源损耗、安全性和扩展性等方面,存在理论研究落后于实践发展、过多集中在比特币环境、一些重要问题尚未涉及、缺乏承载相关研究成果的重要期刊等问题。对此,提出区块链技术的研究者应该加强产学研合作、拓展研究内容、关注未来应用、打造一批重要刊物等建议。

关键词:区块链;比特币;智能合约;加密货币;颠覆性技术

DOI:10.6049/kjjbydc.2017040681

中图分类号:F490.3 **文献标识码**:A **文章编号**:1001-7348(2018)02-0154-07

A Review of Foreign Research of BlockChain Technology

Han Qiuming[1,2], Wang Ge[1]

(1. Chinese Academy of Science and Technology for Development, Peking 100038, China; 2. College of Economic and Social Development, NanKai University, Tianjin 300071, China)

Abstract: Providing a new type of trust mechanism, blockchain technology has a strong catalytic effect and may impact disruptively for a variety of social services. This paper systemizes the international organizations and governments' prejudgment and practice on blockchain technology, and analyzes the research paper of blockchain from web of science literature database. This article finds that the research of blockchain technology mainly focuses on privacy protection, smart contract, resource loss, security and scalability. At the same time, there are several issues like theoretical research lags behind the development of practice, many studies focus on Bitcoin environments, the future development direction is not clear. In this regard, the author proposes blockchain technology researchers should expand the content of research, strengthen cooperation with industry and research, concerns about the future application and other recommendations.

Key Words: Blockchain; Bitcoin; Smart Contract; Crypto Currency; Disruptive Technology

0 引言

在过去几年里,随着对比特币等数字货币探索的深化,信息技术领域的一个重要创新——区块链技术,已成为一个极具潜力的颠覆性技术。区块链技术凭借可共享、可编程、安全可信等特点,对金融交易以及其它社会服务产生巨大影响,已得到各国政府、产业界和科研机构的高度关注。2015 年世界经济论坛发布的《深度转变——技术引爆点与社会影响》指出,在 2025 年前后,全球 GDP 总量的 10%将利用区块链技术存储,同时政府将会使用区块链技术实现税务征收[1]。2016 年 Gartner[2]公司公布了年度新兴技术成熟度曲线,区块链技术与 4D 打印等其它 15 项新兴技术首次进入曲线,并预测其将在 5－10 年内逐渐成熟。OECD 在 2016 年底发布的《科技创新展望 2016》将区块链技术列为十大未来技术发展趋势之一[3]。美国、英国、日本等发达国家对区块链技术持开放态度,如美国证券交易所已批准公司可以基于区块链技术进行股票交易,并且一些州已对区块链技术立法;2016 年初,英国政府发布《分布式账本技术:超越区块链》研究报告,从国家层面对区块链技术的未来发展及应用进行分析并给出建议[4];日本经济产业省于 2015 年召开金融会议,设置专题研究区块链技术的未来发展与影响[5]。

我国区块链技术研究刚起步。尽管在 2013 年底,

收稿日期:2017-06-08

基金项目:科技部创新战略研究专项项目(ZLY2015126);北京科技创新中心建设战略研究及专家咨询专项项目(Z171100003217028)

作者简介:韩秋明(1984－),男,河北石家庄人,博士,中国科学技术发展战略研究院助理研究员,南开大学经济与社会发展研究院联合博士后工作站博士后,研究方向为科技预测与评价;王革(1968－),男,安徽芜湖人,博士,中国科学技术发展战略研究院科技预测与评价研究所所长、研究员,研究方向为科技预测与评价。

我国发布了《关于防范比特币风险的通知》，将比特币定性为非真正意义上的货币，禁止金融机构提供比特币交易服务，但这并不意味着我国关闭了区块链技术的大门。随着区块链技术逐渐在国际上得到认可，吸引了我国政府、产业界和科研机构的关注。在产业层面，区块链应用研究中心、中国区块链研究联盟、中关村区块链产业联盟、中国分布式总账基础协议联盟等一批区块链产业联盟已经建立；在政府层面，央行指出，如果央行发行数字货币，区块链技术将是可以考虑采用的技术之一，并召开数字货币相关研讨会；在研究层面，CNKI 中检索“区块链”显示，我国相关研究数量从 2015 年仅有的 6 篇，到 2016 年剧增至 328 篇。总的来说，我国区块链技术研究还处于萌芽阶段。因此，关注国外区块链技术研究重点，可为我国相关研究提供参考借鉴。

1　区块链技术研究概况

区块链引起人们普遍关注的原因在于其核心属性，即安全性、匿名性和数据完整性，并且不需要任何第三方机构控制相关信息流转。IBM 曾总结出区块链技术的主要特征，即分布式且可持续、安全而持久、透明且可审计、基于共识并可交易，以及经过统筹而灵活[6]。所有网络参与者必须一致认可交易的有效性，这使得区块链技术可以创造交易或资产交换条件。

最早关于区块链技术的论文可以回溯到 2008 年 Satoshi Nakamoto[7] 发表的《Bitcoin：A Peer-to-Peer Electronic Cash System》。在 Web of Science 上以“blockchain”为检索词，时间截止到 2016 年 12 月 31 日，通过主题精确检索方式，可以检索到论文 117 篇，时间分布如图 1 所示。

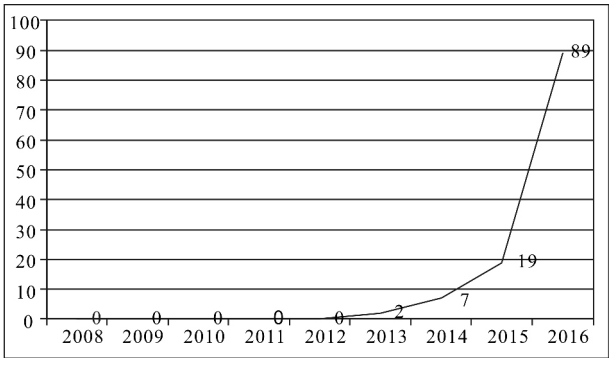

图 1　Web of Science 区块链研究论文的时间分布

从图 1 可以看出，尽管比特币的实践从 2008 年就已开始，并于 2009 年建立了世界上第一个区块链，但关于区块链技术的学术研究从 2013 年才算起步，2015 年后进入快速发展阶段，呈爆发式发展趋势。

从研究的国家看，美国在研究数量上位列第一，截至 2016 年底共有 34 篇文章；其次是英格兰，共发表 11 篇文章；其后是德国，发表 10 篇文章。虽然我国相关研究起步较晚，但也已发表了 8 篇文章，在亚洲处于领先位置。具体情况如图 2 所示。

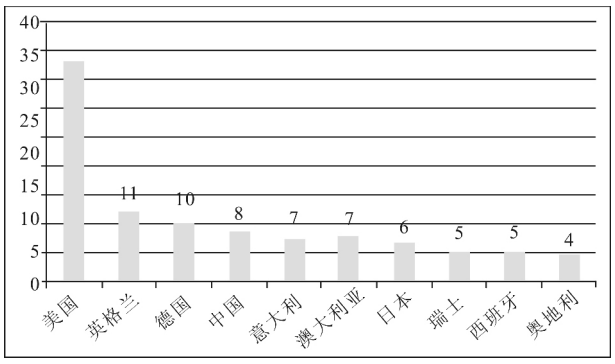

图 2　Web of Science 区块链研究论文发表国家分布

从相关文献的类型看（如表 1 所示），会议论文有 86 篇，期刊论文有 19 篇，工作手稿、新闻条目等占据剩余比例。从文献类型统计结果可知，目前区块链技术在国际上仍处于研究起步期，以会议论文为主，比例约为 73.5%。学术会议是交流新思想、新概念、新技术、新方法的合适载体，一些新的理念尚未成熟，不能形成论文或申请专利，但它也很重要，是未来发展的备选方向之一。当然，研究起步期意味着该技术未来主要发展方向尚不明朗，也许会冲击现有的经济、社会体系，如何平衡各方利益尚未有妥善的办法。因此，相关研究应更多关注潜在影响、未来应用场景等问题。

表 1　Web of Science 区块链研究论文的类型统计

文献类型	数量	比例(%)
Proceedings Paper	86	73.5
Article	19	16.2
Editorial Material	4	3.4
News Item	4	3.4
Letter	2	1.7
Review	1	0.8
Correction	1	0.8

从相关研究的关键词看（如表 2），出现频次较多的是比特币、加密货币、智能合约、以太坊、信任、隐私和安全等，这也是目前区块链技术研究的主要问题。

2　国外区块链技术研究述评

Swan[8] 在其《区块链：新经济的发展蓝图》一文中提出 7 个区块链技术应用的挑战和限制，分别是每秒事务处理量、延迟、规模和带宽、安全性、资源损耗、可用性、分链管理等。对已有文献进行快速浏览，发现大部分讨论内容确实与区块链技术的应用环境、挑战、影响等问题有密切关联。此外，由于区块链技术的匿名

性特征，隐私保护也是一个需要关注的问题。区块链技术的改进和应用也是研究关注的重点，改进是指对当前区块链和比特币技术发展状况提出改进对策、思路和解决方案，应用是指提出区块链技术应用场景[9]。

表 2 Web of Science 区块链研究论文关键词（部分频次≥2 的实词）

关键词	频次
Blockchain（区块链）	42
Bitcoin（比特币）	33
Crypto currency（加密货币）	13
Smart Contract（智能合约）	10
Ethereum（以太坊）	7
Digital currency（数字货币）	3
Trust（信任）	2
Privacy（隐私）	2
Peer-To-Peer（点对点）	2
Cryptographic Protocols（密码协议）	2
Access Control（访问控制）	2
Security（安全）	2

2.1 区块链技术概念讨论

区块链是分布式账本的底层技术，最初是为了在 2008 年实现点对点数字现金系统比特币而设计的。区块链算法让比特币交易可以在“区块”里集中起来，并通过密码签名添加到现有区块组成的“链”中[4]。投资百科（Investopedia）认为，区块链是一个公共分类帐本，所有比特币交易都需要以此为支撑[10]。Anthony Lewis[11]认为区块链是一种既可公用也可私有的分布式数据库。一般来说，区块链技术主要指分布式账本，即在许多计算机之间共享交易的列表，而不是仅仅存储在一台中央服务器中。每一个区块都包含交易信息和数据。Swan[12]对区块链如何发挥作用进行了描述，认为这种比特币交易背后的底层协议为未来如何使物联网发挥更大作用指明了方向，并进一步阐述了区块链协助实现系统完整性、过程完整性、操作完整性的机制。Moser 等[13]正在开发一种适用于金融市场的区块链技术应用框架，认为区块链是一种安全的、具有弹性的架构，可以抵御强大的攻击。

由此可见，区块链技术是在多主体且无需相互信任的条件下，通过去中心化和加密技术，使系统中所有参与者协作，集体记录、维护一个可靠数据库的技术方案。区块链技术使参与到系统中的任意多个主体，将一段时间内系统中全部信息交流数据通过加密算法，计算和记录到一个数据块，并且产生该数据块的密码，用于链接数据链上的下一个数据块并进行校验，同时系统中所有参与主体可以共同认定记录是否为真。从该原理看，未来区块链技术将有无限发展潜力。

2.2 区块链技术隐私保护

由区块链技术的基本原理可知，区块链网络不是由任何一个组织所拥有、管理和控制的，所以它的持续运行并不依赖于任何单独实体。在这种共识的分布式网络上，所有交易都是透明的，并且向公众公开。公众可以看到所有的交易，但是看不到交易的链接和身份信息，这在很大程度上实现了隐私保护与透明交易的平衡。

Herrera-Joancomartí[14]对比特币的匿名性问题作了详细的回顾和总结，作者认为大部分研究人员都将区块链技术视为对隐私保护有天然的作用，只有很少的文献考虑到比特币的交易可能会泄露隐私信息。一些学者还在如何解决区块链技术隐私问题方面提出了建议。Androulaki 等[15]提出了一种系统，它可以通过不可见签名和一种只能由公众添加的日志修改和调整区块链的底层协议，这种日志可以使第三方验证不可见签名的有效性。Ziegeldorf[16]等人提出了一种基于解密混合网络与阈值签名组合的系统。通过对其原型的评估，作者认为这种系统对于那些针对区块链的恶意攻击来说是比较安全的，而且在现实世界的网络中可以较为轻易地扩大参与者的规模。Saxena 等[17]提出了一种完全分散的比特币混合协议，允许用户以真正匿名的方式使用比特币。它不需要任何第三方（信任的、可信赖的或不可信赖的），并且它与当前的比特币系统无缝兼容。这种协议虽然使用户增加了一小部分通信成本，但同时消除了维护匿名所需的费用，并使比特币系统其他消耗（如计算、通信等）的成本最小化。

隐私保护问题十分重要，是区块链技术能否落地应用的关键问题之一。很多国家和机构之所以对隐私保护问题持续关注，就是希望找到一种既能满足监管要求，又不侵害数据隐私的方式。目前产业界已经有了诸如基于 Tear-Off、State Chanell、CCP 等技术的解决方案。以上学者的研究，为如何实现区块链技术的隐私保护作了很多有益的尝试，特别是在比特币这种已经成型并颇具规模的加密货币体系中的隐私保护方案，为下一步的应用提供了很有价值的参考借鉴。

2.3 智能合约

智能合约是密码学家 Nick Szabo[18]在 1994 年率先提出的以数字形式定义的一系列承诺，以及支撑合约参与方执行这些承诺的协议。职能合约一旦设置指令以后，能够无需中介抑或第三方的参与自动开始执行，并且没人任何机构或人可以阻止它的运行。区块链技术为智能合约提供了可信赖的执行环境，而智能合约为区块链扩展了应用范围。

Jesse Yli-Huumo[9]等认为智能合约是利用区块链技术在两个或更多参与者之间创建合同的解决方案。与使用比特币区块链相似，智能合约在分布式环境下完成，当条件触发时，由区块链系统自动执行合约条款。Bigi 等[19]引入了一种分散智能合同协议，并根据

比特币的协议验证了它的可行性。这种协议是博弈理论和形式化模型的组合，作者认为这种分布式智能合约系统是一种非常有前景的方法，值得进一步研究和开发。Wan 等[20]提出了一种在比特币网络使用双方之间的电子签名协议，它可以提供时间戳服务。此外，智能合约还可以根据不同的目的，应用于各种环境和行业之中。比如，Kishigami 等[21]提供了一个基于区块链技术的数字内容发布系统，并公布了概念原型系统。这个系统最具影响力的一点就是为数字权利管理提供了分散化机制。然而，这个系统目前没有对比特币的挖掘计算提供激励机制，这可能也是目前系统能否被采用的主要影响因素。

智能合约是区块链技术最重要的特性之一。区块链技术之所以能够被称为颠覆性技术，智能合约就是其中的一个重要原因。目前世界许多国家的银行考虑使用区块链技术作为发行数字货币的技术基础，智能合约也是其中重要的考量因素。智能合约可能给许多产业带来具颠覆性改变，也许在今后还会对人类社会结构产生重大影响。上述学者对于区块链技术中智能合约的研究，使得该技术从理论研究走向实践应用，并展现出很强的应用潜力，为区块链技术提供了重要支撑。尽管该技术还有一些尚未解决的问题，但显然，更多学者和研究人员的加入会使智能合约技术不断进步、更加完善。

2.4　资源损耗

挖掘比特币需要以可信赖的方式计算和验证交易，而这会消耗大量的电脑运算能力，因而会带来很高的能源消耗。据估计，比特币网络运行所需的能源超过 1GW(10 亿瓦特)，相当于爱尔兰一年的电力消耗。

当然，为了提高开采比特币工作的效率，又不能增大资源损耗是比较困难的。Wang 和 Liu [22]根据独立矿工和矿池数量及生产力介绍了比特币开采的演变历程。在早期，计算能力均匀分布在独立的开采者中。随着比特币网络的发展，矿池的计算能力大幅提升。所有采矿者进行的都是一种零和竞赛，即每一位开采者自身的计算能力提升，那么网络整体计算能力也会得到大幅提升。为此，系统增加了开采难度值，以保持稳定的比特币创建速度，这反过来就降低了个人矿工的比特币开采率。针对资源损耗问题，一些学者提出了一些应对方法。Paul 等[23]通过引入一些额外的字节以更有效地利用时间戳来修改当前区块头，通过计算验证展示了一种使比特币开采能耗降低的新方案。这种方案占用的计算能耗不大，可以算是一种环境友好型方案。Anish[24]提出了实现比特币开采环境更为高速、高效的方法，涉及在采矿池的单个机器中同时使用 CPU 和 GPU。结果表明，大型开采池中的标准开采硬件可以显著增加整体散列率。Barkatullah 等[25]提出，通过使用一种具有高计算能力效率的开采硬件来获得高经济效益的经济模式，并设计了一种比特币开采处理器，介绍了使用这种处理器的开采设备，特别关注于如何解决高功率密度和提高能效的问题。

以区块链技术为底层技术的比特币挖掘，确实会损耗一定的资源，这也是许多学者和产业工作人员批判比特币的理由之一。他们认为比特币非常浪费资源，不环保，消耗了大量电力和运算能力，不是一个“好”的货币，并由此提出“二代数字货币”或者“山寨数字货币”。实际上，比特币开采并非一开始就如此消耗资源。在比特币的初期，只需要普通电脑就可以挖掘，之后随着热度不断蹿升，逐渐演变为一个个大型矿场进行开采。之所以出现这种情况，是因为认同比特币价值的人越来越多，其在市场上的价格不断上升，而价值资源和时间、货币等资源是可以互换的。上述学者的研究表明，目前已经有很多研究人员投入到减少比特币开采的资源损耗中，并且已经取得了一定的进展，可以相信，相应的问题在不久的将来会得到妥善解决。

2.5　安全性

区块链技术使得分布式账本难以被黑客攻击，因为它不是用单一的数据库去存储交易记录，而是在区块上同时保留同一数据库的多个共享副本，因此黑客要想篡改账本信息，必须同时针对所有副本进行攻击才会有效。这个技术也具备阻止未授权修改或恶意篡改的能力，因为区块中的每笔交易都会成为永久记录的一部分，且都有时间戳，参与者可以共享数据，并确保账本的所有副本在任何时候都是与其它副本一致的，可以利用时间戳进行实时验证，若一个账本被篡改，会立刻被发现。当然，这并不是说黑客对区块链技术无计可施，因为从原则上说，任何人只要能够找到“合法地”修改一个副本的方法，就有可能修改账本中的所有副本。因此，保证区块链的安全性是一项重要的任务。

随着比特币等数字货币的认可度逐渐提升，一些个人和机构越来越多地使用比特币进行付款、转账等交易，因此安全事件给比特币用户造成的经济损失有所增加。一些文献明确提出了在比特币网络上发生的安全事件。Vasek 等[26]通过跟踪网上论坛和采访自愿的义务警员，调查了 4 种类型的比特币诈骗(庞氏骗局、开采诈骗、钱包诈骗和交易欺诈)，发现仅 2013－2014 年就有 13 000 受害者，涉及 11 000 000 美元的欺诈。Mougayar 等[27]分析了比特币安全漏洞的趋势及其对策，认为比特币网络可能的安全漏洞包括 DDoS 攻击、使用特洛伊木马的私人帐户黑客或广告中的病毒。作者介绍了对个人用户和比特币交易来说相对安全的

对策，例如硬件钱包和硬件认证设备。Vasek 等[26]在比特币交流论坛上进行了 DDoS 攻击调查，作者发现 DDoS 最常攻击的服务是比特币兑换，其次是采矿池，其中特别是大的采矿池。

安全问题是任何技术在实际应用过程中都必须考虑的问题，特别是在信息社会环境下。目前制约区块链发展的重要阻碍也包含安全问题。尽管区块链技术凭借不可逆、不可篡改等特点被认为是“天生安全”的，但上述学者的研究结果清晰地反映了目前区块链技术在安全性上面还存在一些亟待解决的问题。无论诈骗、漏洞还是 DDos 攻击，区块链技术都存在安全方面的挑战。除了上述学者揭露的安全问题，区块链技术也面临其它安全问题，如私钥丢失、算法缺陷等。私钥丢失相当于主体失去了对区块链上的数据控制权，算法缺陷会导致信息被破解，特别是在未来量子计算机强大运算能力的基础上，算法上的任何微小缺陷都将被无限放大。因此，关于区块链技术安全性问题还将持续探讨和研究下去。

2.6 扩展性

最早对区块链扩展性的界定源于 Swan[8]的表述，他认为比特币的应用程序接口使用起来非常困难。当然这是站在开发者的视角，因为应用程序接口是区块链技术支持其它服务和应用的必需元素。客观来说，区块链是基于一个或多个条件执行的业务规则，智能合约可以内置其中。因此，区块链业务网络能够不断发展、成熟，进而支持各种端到端的业务流程及各种不同的社会服务活动，这也证明了区块链技术大有可为的扩展性。

当前区块链技术是数字货币的底层技术，因而区块链技术用户大部分都是加密数字货币的用户，其可用性也可扩展到加密数字货币领域。从用户视角看，区块链技术的可用性就是区块分析能力。在区块链上，新的区块被开采者不断创造和确认，创造出了一个交易流程环境。因此，有必要开发一些支持工具帮助用户分析整个区块链网络，并提高区块链技术的可用性。目前已经有一些系统可以实现部分功能，如 BitConeView 可以将区块链中的比特币流进行可视化；BitIodine 可以解析区块链，并对这些区块用户进行分类、标记，最后对比特币网络中提取的复杂信息可视化。这两个系统都通过了实验与测试，显示出对区块链分析的有效性[28]。这些系统也可以帮助改善安全性和隐私相关问题。

目前，区块链技术已经在众多应用场景进行了有益尝试，主要分布在交易结算、支付、资产管理、合约、供应链审计、股权交易、元数据管理、房地产管理等领域。此外，该技术在军事领域也有一些尝试，如 DARPA 正在研究区块链能否为保护高度敏感数据提供帮助，并且认可其在军用卫星、核武器等数个场景中的应用潜力[29]。随着社会不断进步，未来区块链技术会将不同场景的业务需求映射到技术方案中，基于这些需求对现有的区块链进行改造、延伸、细分与升级，并且随着监管需求不断增加，对于记录完整性和审计的可视化工作也必不可少。可见，区块链技术的扩展性将更好地发挥作用。

3 结语

区块链技术发展时间不长，特别是学术领域还远未成熟。目前来看，区块链技术同大多数新兴技术一样，将来可能产生的颠覆性影响及问题仍不明确，但这也为研究人员提供了广阔的研究空间。

3.1 国际区块链技术研究存在的问题

通过对国外文献进行梳理，总结出当前研究存在以下问题：

(1)理论研究落后于实践发展。目前，世界各国已经开展了区块链技术实践应用，虽然大部分集中于金融领域，但在其它领域也有所尝试并取得了可喜的进展。此外，一些地区开始为区块链技术立法。不过从理论研究现状看，大多数研究还局限于对技术原理的讨论。对于一项新兴技术，其未来发展的关键不在于技术本身的好坏，而是技术的应用场景、为什么而设、如何应用、应对可能存在的问题的措施等方面。从这个角度看，目前国际上关于区块链技术的研究还落后于实践发展。

(2)大多数研究都集中在比特币环境。区块链技术被定义为金融科技(FinTech)之一，当前的应用方向还是以金融领域为主。如果从支撑实践的角度来说，目前的大多数研究都是在比特币网络中进行的，而极少数其它加密货币也是在比特币网络基础上演变而来，没有脱离这个主体。尽管区块链技术是在比特币环境中首先提出的，但这种技术在其它各种环境中也会有很大的用武之地，并且在实践中已经有所体现。因此，研究区块链技术在其它环境中的作用和机理很有必要，它可以提供和生成更好的交易模型，从而提高区块链技术在不同行业应用的可能性。

(3)一些重要议题尚未涉及。前文已经述及，Swan 曾提出 7 项区块链技术需要突破的限制和挑战。如果从这个角度来说，目前的文献中还缺少对处理性能、扩展性、集成性等主题的研究。当然，这和区块链技术在学术界兴起时间不长有关，学术论文发表周期较长，只能代表 1 年之前的研究内容，但是以上议题的相关研究也应该尽早开展。特别是当前比特币等数字货币的交易数量还远远小于银行货币的交易数量，如果将来

区块链技术在金融行业全面铺开，交易数量会变得极其庞大，那么区块链技术的延迟、带宽以及资源浪费等方面的问题就显得极为重要。

(4)缺乏高质量期刊等出版物。专著、学术期刊等出版物是一个技术领域的学术交流平台，一项技术研究的学术发展依赖于专业出版物的发展，而专业出版物又引领着技术研究的方向，吸引更多研究人员的参与，促进技术领域的人才培养和成长，二者互相促进，相辅相成。目前，大部分关于区块链技术的研究成果发表在交流会、座谈会和研讨会等学术会议上，一些关于区块链的图书也大部分是科普性质，一些高质量、有影响力的期刊和学术专著目前仍然较少。

3.2　研究展望

针对上述问题，下一步研究可以从以下几个方面开展：

(1)加强区块链技术研究的产学研合作。区块链技术是典型的产业驱动型技术，不是凭空诞生的新技术，而是互联网技术演化到一定程度、突破应用阈值后的产物，属于技术的渐进式创新，与实践需求密切相关，因而理论研究或科研创新应该越早越好。针对目理论研究落后于实践发展的现状，下一步应该加强区块链技术产学研合作，在政府宏观管理下，加强企业、产业联盟、开源社区、高校等机构之间的合作，形成共识机制，联合开展研究。

(2)拓展区块链技术研究范围。由于研究起步时间较晚，区块链技术研究还存在很多空白领域。对于具有颠覆性潜力的技术来说(如比特币，将会挑战国家金融管理权威，以及现存全球经济和货币体系)，技术监管、漏洞监测和应急反应、遭遇攻击的后果及责任等问题亟待详细讨论。此外，还有之前提到的计算能力和网络性能等问题(目前公开的比特币区块链只能支持平均每秒约 7 笔的吞吐量，乐观预测不久之后将很快突破每秒数千次的基准线，即使得到大规模应用，仍与现有证券交易系统每秒数万笔的峰值有较大差距)，以及目前已经出现的侧链(side chain)、影子链(shadow chain)、私有链(private chain)等，这些问题都有待深入研究。因此，扩展区块链技术的研究范围十分必要。

(3)关注区块链技术在经济、社会生活中的应用前景。对于新兴技术来说，能否保持生命力受诸多因素影响，关键是否能找到合适的应用场景，但目前对区块链技术的讨论多发生在金融领域。实际上，区块链技术在不引入第三方中介机构的前提下，具有去中心化、不可篡改、安全可靠等特性。因此，所有直接或间接依赖第三方担保信任机构的活动，均有可能从区块链技术中获益。基于这些特点，区块链技术将有可能应用于金融交易、征税、护照管理、土地管理、供应链管理、物联网、网络空间和执法、航运航空管理等领域，确保记录和服务的准确性与安全性。

(4)依托各类学术会议，产生一批高质量、有影响力的出版物。区块链技术研究文献中，超过 70% 的比例发表于各类会议，学术会议已成为讨论、凝聚、汇集相关研究成果的主要载体。因此，可以从价值导向、主题设置、审稿评审、专家邀请等层面策划和举办各类区块链技术研讨会，邀请来自政府、产业、企业、科研院所、高校等不同机构的从业人员和科研人员，从理论、机理、实践、应用场景、未来趋势等多个层次和角度进行探讨，形成高质量、有影响力的出版物，促进相关技术领域的理论研究与实践发展。

综上所述，区块链技术未来的发展对经济社会各领域都极具吸引力，区块链技术的研究主题将随着实践进展而变得丰富。尽管目前研究还处于起步期，但可以确定的是，当区块链技术得到不同行业和学术界更多关注后，将会显现出更大的实践价值。

参考文献：

[1] World economic forum. deep shift-technology tipping points and societal impact. [EB/OL]. http://www3. weforum. org/docs/WEF-GAC15-Technological-Tipping-Points-report-2015. pdf，2017.

[2] GARTNER. 2016 Hype cycle for emerging technologies identifies three key trends that organizations must track to gain competitive advantage. [EB/OL]. http://www. gartner. com/newsroom/id/3412017，2017.

[3] OECD. Science, technology and innovation outlook 2016 [EB/OL]. http://www. ewi-vlaanderen. be/sites/default/files/bestanden/oecd-science-technology-and-innovation-outlook-2016. pdf，2017.

[4] Government office of science. distributed ledger technology：beyond block chain[EB/OL]. https://www. gov. uk/government/uploads/system/uploads/attachment-data/file/492972/gs-16-1-distributed-ledger-technology. pdf，2017.

[5] 唐文剑. 区块链国内外发展快速扫描[J]. 金融电子化，2016(3)：66-68

[6] IBM 商业价值研究院. 全速前进：随着区块链重新思考企业生态系统和经济模式[EB/OL]. https://www-935. ibm. com/services/multimedia/16-Fast-forwardCNZH. pdf，2017.

[7] SATOSHI NAKAMOTO. Bitcoin：a peer-to-peer electronic cash system. [EB/OL]. https://bitcoin. org/bitcoin. pdf，2017.

[8] SWAN M. Blockchain：blueprint for a new economy[EB/OL]. http://w2. blockchain-tec. net/blockchain/blockchain-by-melanie-swan. pdf，2017.

[9] JESSE YLI-HUUMO，DEOKYOON KO，et al. Where is current research on blockchain technology—a systematic re-

view [J]. PLoS ONE 11(10):e0163477. doi:10.1371/journal.pone,0163477.

[10] COINDESK. What is bitcoin retrieved from coindesk[EB/OL]. http://www.coindesk.com/information/what-is-bitcoin/,2017.

[11] LEWIS A. A gentle intorduction to blockchain technology. Retrieved from Bits on blocks[EB/OL]. http://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchaintechnology/,2017.

[12] SWAN M. Blockchain thinking:the brain as a decentralized autonomous corporation[J]. IEEE Technology and Society Magazine,2015(34):41-52.

[13] MOSER M, BOHME R, BREUKER D. An inquiry into money laundering tools in the bitcoin ecosystem[C]. eCrime Researchers Summit (eCRS),2013.

[14] HERRERA-JOANCOMART J. Research and challenges on bitcoin anonymity[EB/OL]. link.springer.com/content/pdf/10.1007%2F978-3-319-17016-9-1.pdf,2017.

[15] ANDROULAKI E, KARAME G. Hiding transaction amounts and balances in bitcoin[EB/OL]. https://pdfs.semanticscholar.org/da9a/85e5 d7b7bd9f43255656558d40989ac23a43.pdf,2017.

[16] ZIEGELDORF J H, GROSSMANN F, et al. Secure multiparty mixing of bitcoins[EB/OL]. https://www.comsys.rwth-aachen.de/fileadmin/papers /2015/2015-ziegeldorf-codaspy-coinparty.pdf,2017.

[17] SAXENA A, MISRA J, DHAR A. Increasing anonymity in bitcoin[EB/OL]. http://fc14.ifca.ai/bitcoin/papers/bitcoin14-submission-19.pdf,2017.

[18] NICHOLAS J,SZABO. Smart contracts[EB/OL]. http://w-uh.com/download/WECSmartContracts.pdf,2017.

[19] BIGI G, BRACCIALI A, MEACCI G, et al. Validation of decentralised smart contracts through game theory and formal methods[EB/OL]. https://dspace.stir.ac.uk/bitstream/1893/23914/1/bHalo-Degano2015.pdf,2017.

[20] WAN Z, DENG R, LEE D. Electronic contract signing without using trusted third party[EB/OL]. https://skbi.smu.edu.sg/sites/default/files/skbife/pdf/asset% 20allocation%20-%20ContractSigning-CR.pdf,2017.

[21] KISHIGAMI J, FUJIMURA S, et al. The blockchain-based digital content distribution system[C]. Big Data and Cloud Computing 2015 IEEE Fifth International Conference ,2015:187-190

[22] WANG L, LIU Y. Exploring miner evolution in bitcoin network.[EB/OL]. http://wan.poly.edu/pam2015/papers/23.pdf,2017.

[23] PAUL G, SARKAR P, MUKHERJEE S. Towards a more democratic mining in bitcoins[EB/OL]. https://link.springer.com/chapter/10. 1007/978-3-319-13841-1-11, 2017.

[24] ANISH DEV J. Bitcoin mining acceleration and performance quantification. in: electrical and computer engineering (CCECE)[C]. 2014 IEEE 27th Canadian Conference , 2014:1-6.

[25] BARKATULLAH J, HANKE T. Goldstrike 1: cointerra's first-generation cryptocurrency mining processor for bitcoin [J]. Micro, IEEE, 2015,35(2):68-76.

[26] VASEK M, MOORE T. There's no free lunch, even using bitcoin: tracking the popularity and profits of virtual currency scams[EB/OL]. http://fc15.ifca.ai/preproceedings/paper-75.pdf,2017.

[27] MOUGAYAR W. Why fragmentation threatens the promise of the blockchain[EB/OL]. http://www.coindesk.com/fragment-blockchain-identity-market/,2017.

[28] SPAGNUOLO M, MAGGI F, ZANERO S. Extracting intelligence from the bitcoin network[EB/OL]. https://www.ifca.ai/fc14/papers/fc14-submission-11.pdf,2017.

[29] 大突破:美国核武器要这么玩——区块链技术控制[EB/OL]. http://news.mydrivers.com/1/502/502939.htm, 2017.

(责任编辑:林思睿)