

# 国外区块链研究主题及展望\*

程晨 张毅\*\* 宁晓静 杨奕

华中科技大学公共管理学院 湖北武汉 430074

**摘要:** 区块链是实现去中心、去中介交易,并构建可信社会的一个新技术范式,围绕区块链进行研究有助于理解、把握信息技术的发展脉络和动态趋势,分析技术范式转变对经济、社会的影响。运用 Citespace 对 Web of Science 核心数据库收录的 233 篇以“区块链”为主题的研究文献进行可视化分析,聚类出行为模式、实现可持续发展目标、比特币协议、用例、区块链技术、拜占庭对手、支付方式、信托法、危险交易等九大热点主题,主要集中在区块链技术价值、区块链技术改进、区块链应用场景、区块链发展挑战等四个方面。最后指出,后续研究可在三个方向进一步拓展和深化,即探讨采纳区块链技术的影响因素,深化探索和构建区块链应用场景、评估区块链应用的综合效益,研究区块链对人类社会的深远影响。

**关键词:** 区块链;比特币;科学计量

**DOI:** 10.16582/j.cnki.dzzw.2018.06.002

## 一、引言

自2008年中本聪<sup>[1]</sup>提出比特币以来,作为第一个全球应用广泛的去中心化数字货币,比特币的发展受到理论界和实务界的关注,并引发其他数字货币的兴起<sup>[2]</sup>。支持比特币发展的底层技术是维护分布式账本的中本聪共识协议,也即区块链<sup>[3]</sup>。区块链是在去中心的点对点网络中,基于加密算法和共识机制等技术原理,记录完整的、带有时间戳的、防篡改的交易记录,并由集体维护交易数据的分布式数据库<sup>[4]</sup>。与传统集中式数据库不同,一方面,区块链没有中心节点,能够在去中介条件下完成交易,因而成本更低、效率更高<sup>[5]</sup>;另一方面,区块链在分布式记录和分布式存储环境下运行,能够保证信息透明、可追溯,并有效解决双重支付和拜占庭将军问题(Byzantine failures)<sup>[6]</sup>。2015年,区块链概念及其应用逐渐走进公众视野,其价值日渐受到重视,相关

研究也呈现出快速发展之势。

由于区块链是信息技术领域一个新兴议题,本文在回顾区块链研究现状后,利用科学文献与知识图谱可视化软件Citespace对国外区块链研究主题进行深入分析,在此基础上提炼出未来区块链研究动态,以期全面了解国外区块链研究的现状和前沿,为进一步开展相关研究积累一定理论基础。

## 二、当前国外区块链研究基本情况

虚拟数字货币比特币凭借着去中心化、匿名、安全等特性,使得低成本、快速验证在线交易成为可能<sup>[7]</sup>,而维系比特币系统稳定运行的支撑技术——区块链,日渐引起学界的关注。学者们纷纷从技术、经济、法律、商业、监管等视角对区块链展开研究和探讨<sup>[8]</sup>,积极尝试推动区块链与比特币之外的其他领域相融合,探索区

\* 基金项目:国家自然科学基金项目“基于大数据的公共价值挖掘与公共决策支持研究”(项目编号:71573096);华中科技大学自主创新研究基金项目“区块链与基于技术信任的政府治理创新”(项目编号:2017WKZDJC005)。

\*\* 通讯作者 收稿日期:2018-03-08 修回日期:2018-04-08

区块链多元化应用,以实现在安全、透明、隐私保护的价值转移的同时<sup>[9]</sup>,促进去中心化、去中介化的社会信任关系构建<sup>[10, 11]</sup>。正是在这样的发展态势下,当前形成了不同学科、不同领域对区块链研究的发展脉络和知识谱系。

本项研究借助Web of Science (WoS) 数据库和Citespace可视化分析工具,对区块链现有研究进行梳理和分析。基于WoS数据库,设定检索条件为“数据库=Web of Science核心合集”“主题=blockchain”,共计检索到233篇英文文献,作为本文的数据来源(截至2017年10月19日)。然后,利用科学文献与知识图谱可视化软件Citespace对233篇文献进行可视化分析,以揭示当前区块链研究现状和发展概况。

### (一) 区块链研究的时序分布

总体来看,虽然当前的区块链研究已在全球范围内成为热点和焦点,但是面向理论研究和应用创新的区块链研究仍处于起步阶段。WoS中区块链相关论文自2013年开始出现,2016年开始迅速增多,截至数据收集日期,2017年已发表论文量接近上一年,并呈现持续增长

趋势(参见图1)。

具体而言,尽管比特币区块链的研究发轫于中本聪发表于2008年的奠基之作,但相关学术成果始于2013年<sup>[12]</sup>,这一方面反映人们对底层技术认识是由浅入深的过程,另一方面也突出区块链的价值是逐渐显现的。早期文献大多聚焦于比特币的发展,2013年到2015年期间发表的文献,大多数是从介绍比特币及其系统网络出发,分析系统运行中挖矿激励问题<sup>[13, 14]</sup>、延缓问题<sup>[15]</sup>、诸如洗钱等非法活动问题<sup>[16]</sup>以及法律和伦理问题<sup>[17]</sup>,对比特币背后的广播机制、验证机制、分布式加密技术原理<sup>[18, 19]</sup>等进行探讨和改进,有学者还借助“技术接受模型”阐释比特币应用的可用性和易用性问题<sup>[20]</sup>,尝试探究区块链相关应用。初期研究为后续学者提供有关区块链的基础知识,也标志着区块链向多领域的外溢。2016年,各国政府相继开启区块链技术探索,相关文献数量迸发,其研究范围涵盖更加全面的区块链技术原理剖析,挖掘基于区块链更多样化的应用场景。这一年,区块链首次进入Gartner曲线并跃居期望线顶端<sup>[21]</sup>,人们也将2016年称作“区块链元年”。

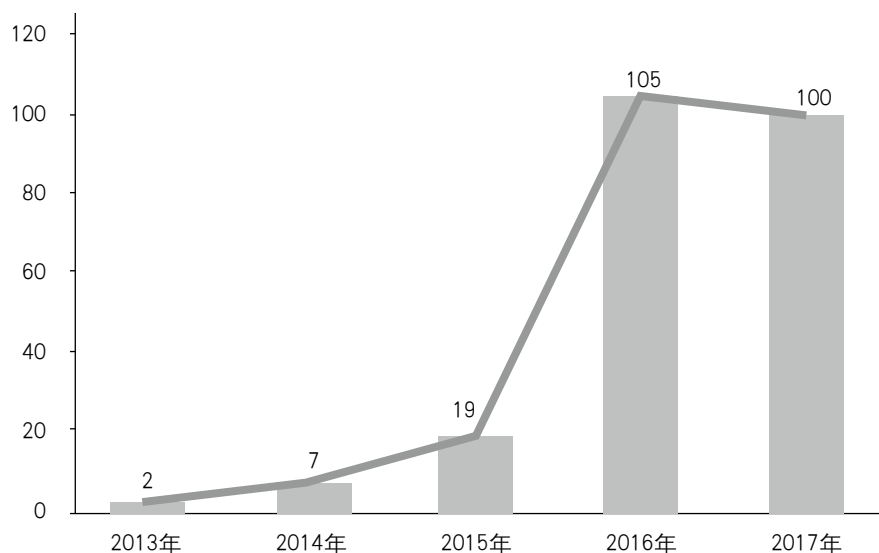


图1 区块链相关论文发表量的时序分布

## (二) 区块链研究的学科领域

利用Citespace生成学科类别贡献图谱,以把握现有研究的知识结构及其演变。根据节点“中间中心度>0.1”的原则,识别出当前研究“区块链”的主要学科类别(参见表1)。

不难看出,区块链相关研究日益向全方位多学科发展,现有研究主要是以计算机科学、工程学、经济学等学科类别为主,相关学者致力于剖析区块链技术原理,考察区块链对金融业的影响,构建区块链在金融领域的创新应用<sup>[12]</sup>。同时,区块链在能源方面的研究日渐成为关键节点,学者们试图利用区块链来建立新的能源范式,以提升能源利用效率<sup>[22]</sup>。此外,随着区块链应用的丰富化,政府与法学、管理学、环境科学、生态学、行政管理等多学科也相继加入区块链研究行列。学科间的交叉、跨领域间的合作逐渐构筑起区块链研究的合作网络谱图,也体现区块链技术及其应用的广度和多样性。

## (三) 区块链研究共被引聚类网络

共引图谱能够分析区块链研究的知识基础和研究前沿。利用Citespace生成图2,反映区块链研究九大聚类主题的共被引网络时间线视图,其中,施引文献的共被引网络体现一个领域的知识基础,而聚类分析能够提炼这一领域的研究热点<sup>[23]</sup>。

一方面,横轴表示时间维度上各聚类形成的知识基础。圆圈越大,表示该学者在这一时期的影响力越大,2013年前的被引文献以中本聪论文为突发节点,该论文被其他共引文献引用达到73次,表明该文不仅揭开了区块链研究序幕,更是开展相关研究的理论基础。2013年以后,出现以Dorit Ron、Fergal Reid等学者的文献为代表的多个关键节点,逐渐形成区块链研究的知识网络。

另一方面,纵轴表示区块链研究的九大聚类前沿主题,分别是行为模式(behavior pattern)、实现可持续发展目标(achieve sustainable development

表1 区块链研究中心度>0.1的学科类别及其代表文献

规模	中心度	学科类别	代表文献
25	0.63	计算机科学 跨学科应用	Kishigami J等,基于区块链的数字内容分布式系统(2015) Baur A W等,颠覆性的加密货币?有关比特币和Co的用户采纳和未来潜力实证研究(2015)
47	0.36	工程学	Christidis K等,发展物联网的区块链和智能合约(2016) Kosba A等, Hawk:加密区块链模型及隐私保护智能合约(2016)
24	0.26	经济学	Fanning K等,区块链及其对金融服务的影响(2016) Adams R等,金钱的未来和区块链的未来应用(2017)
7	0.24	商业管理学	Tapscott D等,区块链如何变革组织(2017)
32	0.17	电信学	Karame G O,关于比特币区块链的安全性和可扩展性(2016) Lee J H等,区块链革命如何重塑消费电子行业
73	0.16	计算机科学 信息系统	Hari A等,互联网区块链:互联网的分布式、防篡改事务框架(2016) Kraft D,基于区块链共识系统的难度控制(2016)
14	0.14	科学与技术	Cha S C,关于Android应用程序基于区块链声誉服务的设计(2017) Cocco L,比特币市场采矿经济学的建模与仿真(2016)
4	0.14	能源学	Green J,公民事业:新兴的能源范式(2017) Sikorski J J,化学工业中的区块链技术:M2M电机市场(2017)

资料来源:根据Citespace学科类别共引图谱整理

程晨 张毅 宁晓静 杨奕 · 国外区块链研究主题及展望

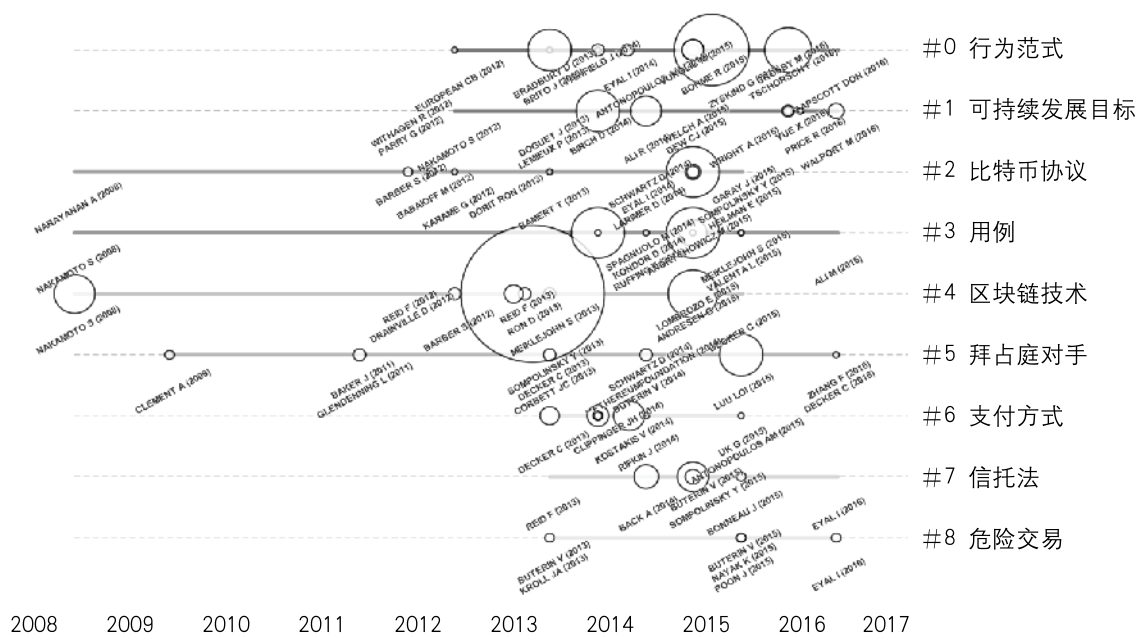


图2 区块链研究九大聚类主题的共被引网络时间线

target)、比特币协议(bitcoin protocol)、用例(use case)、区块链技术(blockchain technology)、拜占庭对手(byzantine adversaries)、支付方式(payment method)、信托法(trust law)、危险交易(poison transaction),反映当前区块链不同的研究方向和重点。九大聚类平均出版年为2013或2014年,聚类轮廓值均在0.7以上,表示聚类合理。这些前沿主题代表了当前学者们对区块链研究的热点所在,揭示出当前研究旨在剖析区块链背后的各种技术原理和机制,挖掘区块链技术的实践价值,同时鉴别应用区块链会带来的相关法律和道德问题。

### 三、当前国外区块链研究的主要议题

在共被引图谱聚类的九项主题分析中,有关实现拜占庭容错、可持续发展方面的研究强调区块链技术对经济社会的深远影响,有关优化比特币协议、节点行为模式、区块链相关技术等主题研究探讨区块链技术系统的

改进,有关重塑支付方式、构建多样化用例的研究阐述了区块链在各个领域的不同应用,有关信托法、危险交易等主题的研究侧重于区块链发展带来的法律和监管问题。总体来看,这些研究从区块链技术价值、区块链技术改进、区块链应用场景,区块链发展挑战等方面综合反映了区块链研究的关键内容。

#### (一) 区块链技术价值

对区块链及相关支撑技术的分析,学者们着重围绕着区块链技术对可编程货币、可编程金融和可编程社会的作用机理和影响机制,挖掘区块链背后蕴藏的技术价值,以促进经济社会发展。

一是分布式架构能够破解集中式或分层式“星型”架构信息不对称难题,实现去中心“网状”结构的网络信息经济<sup>[24]</sup>。以比特币区块链为代表,其能够实现新自由主义学者弗里德里希·哈耶克和米尔顿·弗里德曼提倡的终止由国家(通过中央银行)垄断金钱发行和分配的局面,或实现自由主义学派减少政府对经济控制的理



想<sup>[25]</sup>。一方面, 加密算法、共识机制通过构建去中心、无需信任、冗余的区块链网络架构, 从而创造安全、透明、可信环境, 能够在实现快速交易的同时, 变革现存交易方式, 并保证交易信息的完整性和可追溯<sup>[26]</sup>。例如, 智能合约能够在执行数字协议过程中实现高度自动化, 从而在监控、执行速度和成本方面优势明显<sup>[27]</sup>。另一方面, 通过数字签名、时间戳和工作量证明等, 全网节点共同参与记录能够有效解决数字货币存在的双重支付问题<sup>[4]</sup>, 以及信息不对称产生的拜占庭将军问题<sup>[6]</sup>。

二是推动信息互联网向价值互联网转变<sup>[28]</sup>。互联网搭建起全球范围内在线沟通和协作平台, 能够提供实时信息解决方案, 实现信息的传递和存储, 但是却无法解决价值的交换、转移和存储<sup>[6]</sup>。而基于去中心架构的区块链算法信任能够在去中介的同时构建起“价值互联网”, 对从出生证明开始, 到教育资格证明、社会保障卡、贷款等人类一切价值行为进行编码记录, 实现价值的存储、转移、交易及管理<sup>[29]</sup>, 提供即时的价值解决方案。也就是说, 区块链能够以低成本解决价值交易活动中的信任难题, 实现在去中介下对实物资产和数字资产等的追溯和认证<sup>[30]</sup>, 为围绕价值开展的活动开辟了一系列新的可能。

三是重塑产业形态、商业模式和价值体系, 促进可持续发展。区块链代表革命性和颠覆式创新技术, 去中心和“去信任”特征使得其与大数据、物联网、云计算、人工智能等技术相结合, 能够促进双边信任向多边信任或社会公信的转变<sup>[31]</sup>, 从而带来众多行业变革, 促进传统业务流程再造, 重塑或培育新的商业模式和产业形态<sup>[32, 33]</sup>, 推动工业经济向信息经济的跨越式发展, 继而有助于构建多元价值体系生态系统<sup>[34]</sup>, 甚至形成区块链思维<sup>[35]</sup>。更进一步, 通过考察区块链系统的经济效率、服务效率和运营效率<sup>[36]</sup>, 及其在社会、经济、生态

等多领域应用的可行性, 区块链技术被视作是实现联合国“2030年可持续发展目标”的可行催化剂<sup>[37]</sup>, 有益于结束贫困、保护全球生态系统、实现共同繁荣<sup>[38]</sup>。

## (二) 区块链技术改进

随着区块链技术价值的突显, 部署区块链还面临着一些现实的技术难题。在当前的研究中, 学者们尤其关注区块链系统运行的隐私安全、效率受限两方面的问题, 并提出了相应的技术改进和性能提升方案。

第一, 区块链隐私安全。利用假名等方法保护用户信息的比特币区块链仍然存在数据泄漏的安全隐患。在应用区块链技术时, 达世币(Dash)使用的混币原理(CoinJoin)、门罗币(Monero)使用的环签名(ring)以及零币(Zcash)使用的零知识证明(ZKPs)等方式被用于解决区块链中的隐私保护问题<sup>[39]</sup>。例如, 通过复合签名技术消除或模糊交易发送方与接收方之间的链接, 来增强区块链系统中交易的匿名性<sup>[40]</sup>; 通过椭圆曲线离散对数问题、双线性映射和聚类签名等加密技术提出针对区块链上交易的新签名方案以隐藏交易金额<sup>[39]</sup>; 通过提供分布式架构中保护交易信息的可编程系统Hawk, 利用零知识证明加密原语自动生成加密协议<sup>[41]</sup>, 来实施“无脚本智能合约”, 以支持“跨链交易”智能合约的执行<sup>[42]</sup>, 在保证用户隐私的同时维护区块链系统的稳定。

第二, 区块链运行效率。针对技术本身局限, 提出了基于区块链信任机制的可扩展协议Bitcoin-NG, 能够在容忍拜占庭问题、保障系统安全可信的同时, 实现比特币区块链更高的吞吐量和更低的延迟<sup>[2]</sup>。针对节点运行效率, 提出BPC行为模式聚类算法, 根据区块链网络中节点行为进行自动聚类以节省全网节点耗费的算力成本, 识别网络中异常行为节点, 管理和维护区块链系统<sup>[5]</sup>; 通过使用多重签名方法, 解决无钥匙签名基础设

施(KSI)中日历根散列公布时间低效率问题,并保证交易的灵活、安全<sup>[43]</sup>。针对系统稳定性,将比特币挖矿建模为具有时间依赖性的泊松过程,针对区块哈希增长率情况,通过提升挖矿难度来保证区块链系统的稳定性。此外,学者们通过提出记录完整性证明方案<sup>[44]</sup>、实施可选择的智能合约<sup>[45]</sup>,将区块链、物联网、机器学习算法、人工智能等相融合<sup>[46]</sup>,对区块链技术进行优化和完善。

### (三) 区块链应用场景

区块链中蕴含的巨大产业空间价值、科学研究价值、社会发展价值正在被认知与开发利用,区块链技术及其多元应用超越了国家发展水平和意识形态差异限制,其不仅适用于发达国家也适用于发展中国家<sup>[38]</sup>,不仅适用于资本主义社会也适合应用于社会主义社会<sup>[47]</sup>。梅兰妮·斯万将区块链革新应用分为:区块链1.0、区块链2.0、区块链3.0<sup>[48]</sup>。也就是说从比特币开始,区块链能在金融创新、产业发展、公共管理等诸多领域得到应用。

在金融发展和创新方面,区块链是简化金融机构间交易程序,降低跨国间支付费用、监管成本,提高金融衍生品交易效率的突破口。以去中心化打破组织间信息交换壁垒,以智能合约实现跨区域、跨组织间交易,以加密算法保障用户隐私安全,使得区块链技术具有优化全球金融基础设施的潜力<sup>[36]</sup>,能够提高从贸易融资到支付结算等整个金融体系的效率。当前,以R3区块链联盟为代表的金融服务机构尝试提供区块链即服务(BaaS),包括巴克莱银行、瑞士信贷银行、汇丰银行等在内的成员希望通过使用区块链协议,利用分布式账本、智能合约来提供即时的金融交易服务<sup>[49]</sup>。

在产业发展和规划方面,区块链是重塑产业形态、优化产业生态系统的重要推手。学者们围绕区块链技术

价值构建与农业、工业、服务业等多产业应用场景。以消费电子产业为例,区块链迎合了消费电子产业供应链管理对于信息透明、多元主体参与的需求,能够在全球生产者、消费者共同参与的情况下验证并追溯产业价值链全过程数据和信息的真实性,使得电子产业发展更加透明、安全<sup>[50]</sup>。与此同时,将区块链技术嵌入制造业,能够保证研发、制造、销售全流程项目记录和信息处理的鲁棒性和完整性,弥补传统业务流程中防伪措施的不足<sup>[51]</sup>。此外,依托区块链技术构建数字艺术<sup>[52]</sup>、网络记录<sup>[24]</sup>等新型互联网产业的版权管理系统,能够保障版权所有者信息的准确性和可用性,降低版权管理费用,形成正向激励的产业发展生态。

在社会保障和教育方面,区块链是提供民生服务、完善教育机制的助推器。一方面,针对当前医疗卫生系统之间数据信息存储分散、患者数据隐私被侵犯等问题,学者们提出基于区块链的医疗记录分布式架构模型OmniPHR<sup>[53]</sup>、医疗数据网关HGD<sup>[54]</sup>、MedRec电子病历<sup>[55]</sup>等去中心化自治系统<sup>[56]</sup>,将区块链技术与医疗保健相结合,确保患者掌握个人医疗数据,且在隐私信息得到保护的同时,共享医疗数据,提升医疗服务质量。另一方面,区块链应用于教育界,能够解决学历资格造假、学术同行评审不规范等问题。例如,通过构建区块链架构的学术同行评审代币系统,激励学者提高学术论文评价的质量和规范性,并依托完整的区块链记录对学术评审的进度和责任进行有效追踪<sup>[57]</sup>。

在公共管理和服务方面,区块链是构建智慧城市发展框架、推动政府治理创新的重要支撑。围绕智慧城市发展,学者们将区块链与物联网、共享经济结合,构建智慧交通、智慧家庭、智慧能源、智慧政府等多元应用场景。例如,提出Block-VN模型,将区块链技术引入智慧城市车辆网络结构的优化和管理,提升交通管理的透

明性、安全性<sup>[58]</sup>；在家庭嵌入物联网过程中引入区块链挖矿机制、加密机制，保证智慧家庭信息的保密性、完整性和可用性<sup>[59]</sup>；利用区块链来构建分布式双向能源系统，促进电力资源等能源从集中式管理转变为民主化去中心的多主体参与管理<sup>[22]</sup>。此外，区块链作为自动执行智能合约的引擎能够应用于电子投票<sup>[60]</sup>、政府治理<sup>[25]</sup>等方面，其通过降低交易成本，解决委托代理和道德困境问题来减少官僚作风、抑制腐败<sup>[61]</sup>，提高政府工作透明度、增强选民信心、提升政府公信力和公共管理水平。

#### （四）区块链发展带来的挑战

隐藏在区块链具体应用背后的技术问题、道德困境和监管挑战冲击着其效力的实现。从学者们的研究来看，成功部署区块链，主要面临着来自系统本身的局限性和应用技术的社会环境两方面的挑战。

第一，区块链系统运行自身的挑战。区块可扩展性、数据隐私、互操作性、区块链安全、分叉问题制约着区块链技术应用<sup>[38]</sup>。一方面，吞吐量和延缓问题限制了区块链技术采纳和应用。相比VISA每秒的平均交易量在2000笔而言，比特币区块链需要10分钟左右来确认交易，且吞吐量只能达每秒7笔<sup>[62]</sup>，区块扩容和提高“即时确认”效率成为区块链实现高频交易的一个棘手问题。另一方面，系统风险、操作风险等安全因素阻碍区块链应用。尽管51%的算力难度保证系统的安全性，使得其不易被攻击，但面对矿工采取自私挖矿策略<sup>[13]</sup>以及恶意攻击造成钱包信息泄漏<sup>[32]</sup>、软件版本更新带来的分叉<sup>[63]</sup>等安全问题仍然是区块链技术重大挑战。此外，由高算力需求而产生大量能耗，硬件的高成本带来的资源浪费现象也不容忽视<sup>[36, 64]</sup>。

第二，区块链应用实践中面临的挑战。隐藏在网络空间下的“丝绸之路”网站利用比特币从事洗钱、毒品交易活动<sup>[65]</sup>，Mt. Gox被攻击导致比特币失窃及其破产<sup>[66]</sup>

等事件，为投资比特币的人们敲响警钟的同时也引发有关应用区块链这一底层技术的反思。一方面，区块链架构在理论和实践上冲击着传统法律范式<sup>[67]</sup>。针对区块链应用带来的虚拟与现实之间法律空白问题，一些国家开始采取行动。例如，美国联邦和州的相关监管机构针对区块链货币存在的基本风险实行司法管辖权，美国财政部金融犯罪执法系统FinCEN、纽约州数字货币公司监管框架BitLicense来规范“虚拟货币业务”<sup>[68]</sup>；英国对包括区块链在内的FinTech实施沙箱监管机制<sup>[29]</sup>。但就目前而言，公有链如何形成一个全球治理体系还有待探索。另一方面，区块链应用还受到文化、道德的约束。克兰兹伯格技术六定律中第一条指出：“技术既无好坏，亦非中立。”<sup>[37]</sup>技术应用在不同的社会文化中会带来不同的结果，同时，技术的可用性和易用性也决定了人们对该技术的接受程度<sup>[20]</sup>。区块链应用的一大挑战在于普通人难以理解和掌握智能合约的编码语言和挖矿技术<sup>[27]</sup>，而知识水平的差距可能会重现费恩伯格所谓的“技术特权”，也即技术进步并没有带来民主的进步<sup>[25]</sup>，反而是加剧贫富差距、削弱民主，带来社会不平等现象<sup>[69]</sup>。

#### 四、未来区块链研究展望

区块链是一个兼具学理价值和实践意义的新兴研究领域。学者们从技术、工程、管理、哲学等视角对区块链技术特性及其应用展开了相关研究。具体而言，国外区块链研究呈现如下特征：一方面，当前区块链学术研究处于方兴未艾之势。尽管区块链相关研究还处于起步阶段，但是日渐成为多学科多领域的一个重要课题，并呈现出多学科交叉融合发展态势。另一方面，国外区块链研究主要议题包括行为模式、实现可持续发展目标、比特币协议、用例、区块链技术、拜占庭对手、支付方式、信托法、危险交易等九大主题，集中于区块链技术

价值、技术改进、应用场景和发展挑战等四个方面。

通过分析国外区块链研究的主要议题,今后区块链研究工作可以围绕以下方面扩展和深化:第一,探讨采纳区块链技术的影响因素。已有学者借助技术接受模型,围绕感知有用性和感知易用性<sup>[20]</sup>,分析影响区块链应用的经济和技术方面因素,后续研究可以在前人基础上结合T-O-E模型(技术因素、组织因素、环境因素),从多维动态视角关注影响区块链技术采纳的综合因素及其作用机理。第二,深化探索和构建区块链应用场景。区块链应用起源于数字货币,发迹于金融领域,今后还将拓展到政府、社会等人类世界的各个角落,区块链同其他信息技术一样成为人类社会的重要组成部分。第三,评估区块链应用的综合效益,研究区块链对人类社会的深远影响。例如,基于TCO的信息系统“成本—收益”分析方法对区块链应用场景的效益进行实时测量,比较区块链应用前后的经济效益、社会效益,评估区块链技术的应用价值。探讨区块链技术如何通过去中介、去信任方式将社会信任关系的构建从制度信任向技术信任转变。

### 参考文献:

- [1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. (2008-11-30)[2018-03-18]. <https://bitcoin.org/bitcoin.pdf>.
- [2] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-NG: A scalable blockchain rotocol[C]. 13th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, CA, 2016: 45-59.
- [3] Hurlburt G. Might the blockchain outlive bitcoin[J]. IT Professional, 2016, 18(02): 12-16.
- [4] Tschorsch F, Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies[J]. IEEE Communications Surveys and Tutorials, 2016, 18(03): 2084-2123.
- [5] Huang B, Liu Z, Chen J, et al. Behavior pattern clustering in blockchain networks[J]. Multimedia Tools & Applications, 2017, 76(19): 20099-20110.
- [6] Adams R, Parry G, Godsiff P, et al. The future of money and further applications of the blockchain[J]. Strategic Change, 2017, 26(05): 417-422.
- [7] Peters G W, Panayi E, Chapelle A, et al. Trends in crypto-currencies and blockchain technologies: a monetary theory and regulation perspective[J]. Cryptography and Security, 2015, 3(03): 92-113.
- [8] Ylihuomo J, Ko D, Choi S, et al. Where is current research on blockchain technology? — A systematic review[J]. PLOS ONE, 2016, 11(10), DOI: 10.1371/journal.pone.0163477.
- [9] Tapscott D, Tapscott A. How blockchain will change organizations[J]. MIT Sloan Management Review, 2017, 58(02): 10-13.
- [10] Weber I, Xu X, Riveret R, et al. Untrusted business process monitoring and execution using blockchain[C]//LaRosa M, Loos P, Pastor O. Lecture Notes in Computer Science. Rio de Janeiro, Brazil. Springer, 2016: 329-347.
- [11] Pierro M D. What is the blockchain?[J]. Computing in Science & Engineering, 2017, 19(05): 92-95.
- [12] White G. Future applications of blockchain in business and management: a delphi study[J]. Strategic Change, 2017, 26(05): 439-451.
- [13] Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable[C]//Christin N, SafaviNaini R. Lecture Notes in Computer Science, Barbados. Springer, 2013: 436-454.
- [14] Dev J A. Bitcoin mining acceleration and performance quantification[C]. Canadian Conference on Electrical and Computer Engineering. Toronto, Canada, IEEE, 2014: 1-6.



- [15] Monaco J V. Identifying bitcoin users by transaction behavior[C]//Kakadiaris I A, Kumar A, Scheirer W J. Proceedings of SPIE. Baltimore, Maryland, SPIE, 2015. DOI: 10.1117/12.2177039.
- [16] Moeser M, Boehme R, Breuker D. An inquiry into money laundering tools in the bitcoin ecosystem[C]//ECrime Researchers Summit. San Francisco, CA, IEEE, 2013. DOI: 10.1109/eCRS.2013.6805780.
- [17] Godsiff P. Bitcoin: Bubble or blockchain[C]//Jezic G, Howlett R J, Jain L C. Smart Innovation Systems and Technologies. Sorrento, Italy. Springer, 2015: 191–203.
- [18] Feld S, Schonfeld M, Werner M, et al. Analyzing the deployment of bitcoin's P2P network under an AS-level perspective[C]//Shakshuki E, Yasar A. Procedia Computer Science, Hasselt, Belgium, Elsevier, 2014: 1121–1126.
- [19] Wang L, Liu Y. Exploring miner evolution in bitcoin network[C]//Mirkovic J, Liu Y. Lecture Notes in Computer Science, New York. Springer, 2015: 290–302.
- [20] Baur A W, Bühler J, Bick M, et al. Cryptocurrencies as a disruption? Empirical findings on user adoption and future potential of bitcoin and co[C]//Janssen M, et al. Lecture Notes in Computer Science, Delft Univ Technol. Springer, 2015: 63–80.
- [21] Kewell B, Ward M P. Blockchain futures: With or without Bitcoin[J]. Strategic Change, 2017, 26(05): 491–498.
- [22] Green J, Newman P. Citizen utilities: The emerging power paradigm[J]. Energy Policy, 2017, 105: 283–293.
- [23] Chen C. CiteSpace II: Detecting and visualizing emerging trends and transient patterns in scientific literature[J]. Journal of the Association for Information Science and Technology, 2006, 57(03): 359–377.
- [24] O'dair M, Beaven Z. The networked record industry: How blockchain technology could transform the record industry[J]. Strategic Change, 2017, 26(05): 471–480.
- [25] Filippi P D, Loveluck B. The invisible politics of bitcoin: Governance crisis of a decentralized infrastructure[J]. Social Science Electronic Publishing, 2016, 5(03), DOI: 10.14763/2016.3.427.
- [26] Seebacher S, Schüritz R. Blockchain technology as an enabler of service systems: A structured literature review[C]//Za S, Dragoicea M, Cavallari M. Lecture Notes in Business Information Processing. Rome, Italy. Springer, 2017: 12–23.
- [27] Cuccuru P. Beyond bitcoin: An early overview on smart contracts[J]. International Journal of Law & Information Technology, 2017, 25(03): 179–195.
- [28] Zhao H W, Zhang Y, Peng Y, et al. Lightweight backup and efficient recovery scheme for health blockchain keys[C]. 13th IEEE International Symposium on Autonomous Decentralized System, Bangkok, Thailand, 2017: 229–234.
- [29] Primm H. Regulating the blockchain revolution: A financial industry transformation[J]. Review of Banking & Financial Law, 2016, 36(01): 75–92.
- [30] Nofer M, Gomber P, Hinz O, et al. Blockchain[J]. Business & Information Systems Engineering, 2017, 59(03): 183–187.
- [31] Tapscott D, Tapscott A. Blockchain revolution: How the technology behind bitcoin is changing money, business and the world[M]. Beijing: China CITIC Press, 2016: 12.
- [32] Jin P, Park J. Blockchain security in cloud computing: Use Cases, challenges, and solutions[J]. Symmetry, 2017, 9(08): 1–13.
- [33] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things[J]. IEEE Access, 2016, 4: 2292–2303.
- [34] Pazaitis A, Filippi P D, Kostakis V. Blockchain and value systems in the sharing economy: The illustrative case of Backfeed[J]. Technological Forecasting & Social Change, 2017, 125: 105–115.
- [35] Swan M. Blockchain thinking: The brain as a

- decentralized autonomous corporation[commentary][J]. IEEE Technology & Society Magazine, 2015, 34(04): 41–52.
- [36]Cocco L, Pinna A, Marchesi M. Banking on blockchain: costs savings thanks to the blockchain technology[J]. Future Internet, 2017, 9(03): 25. DOI: 10.3390/fi9030025.
- [37]Kewell B, Adams R, Parry G. Blockchain for good?[J]. Strategic Change, 2017, 26(05): 429–437.
- [38]Underwood S. Blockchain beyond bitcoin[J]. Communications of The ACM, 2016, 59(11): 15–17.
- [39]Yuan C, Xu M X, Si X M. Research on a new signature scheme on blockchain[J]. Security and Communication Networks, 2017(02): 1–10.
- [40]Saxena A, Misra J, Dhar A, et al. Increasing anonymity in bitcoin[C]//Bohme R. Lecture Notes in Computer Science, Christ Church, Barbados. Springer, 2014: 122–139.
- [41]Kosba A E, Miller A J, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[C]//IEEE Symposium on Security and Privacy. San Jose, CA, IEEE, 2016: 839–858.
- [42]Banasik W, Dziembowski S, Malinowski D, et al. Efficient zero-knowledge contingent payments in cryptocurrencies without scripts[C]//Askoxylakis I. Lecture Notes in Computer Science, Heraklion, Greece. Springer, 2016: 261–280.
- [43]Jämthagen C, Hell M. Blockchain-based publishing layer for the keyless signing infrastructure[C]. Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress, Toulouse, France, IEEE, 2017: 374–381.
- [44]Cucurull J, Puiggalí J. Distributed immutabilization of secure logs[C]//Barthe G. Lecture Notes in Computer Science, Heraklion, Greece. Springer, 2016: 122–137.
- [45]Swan M. Blockchain temporality: Smart contract time specifiability with blocktime[C]//Alferes J J. Lecture Notes in Computer Science, Stony Brook, NY. Springer, 2016: 184–196.
- [46]Outchakoucht A, Es-samaali H, Philippe J. Dynamic access control policy based on blockchain and machine learning for the internet of things[J]. International Journal of Advanced Computer Science & Applications, 2017, 8(07): 417–424.
- [47]Huckle S, White M. Socialism and the blockchain[J]. Future Internet, 2016, 8(04): 49. DOI: 10.3390/fi8040049.
- [48]Swan M. Blockchain: Blueprint for a new economy[M]. USA: O'Reilly Media, Inc., 2015: 34–36.
- [49]Fanning K, Centers D P. Blockchain and its coming impact on financial services[J]. Journal of Corporate Accounting & Finance, 2016, 27(05): 53–57.
- [50]Lee J H, Pilkington M. How the blockchain revolution will reshape the consumer electronics industry [future directions] [J]. IEEE Consumer Electronics Magazine, 2017, 6(03): 19–23.
- [51]Kennedy Z C, Stephenson D E, Christ J F, et al. Enhanced anti-counterfeiting measures for additive manufacturing: Coupling lanthanide nanomaterial chemical signatures with blockchain technology[J]. Journal of Materials Chemistry C, 2017, 5(37): 9570–9578.
- [52]Mcconaghy M, McMullen G, Parry G, et al. Visibility and digital art: Blockchain as an ownership layer on the Internet[J]. Strategic Change, 2017, 26(05): 461–470.
- [53]Roehrs A, Da C C, Rosa Righi R D. OmniPHR: A distributed architecture model to integrate personal health records[J]. Journal of Biomedical Informatics, 2017, 71: 70–81.
- [54]Yue X, Wang H, Jin D, et al. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control[J]. Journal of Medical Systems, 2016,

- 40(10): 218. DOI: 10.1007/s10916-016-0574-6.
- [55]Azaria A, Ekblaw A, Vieira T, et al. MedRec: Using blockchain for medical data access and permission management[C]. International Conference on Open and Big Data, Vienna, Austria, 2016: 25-30.
- [56]Garrod, J Z. The real world of the decentralized autonomous society[J]. Triplec-Communication Capitalism& Critique. 2016, 14(01): 62-77.
- [57]Spearpoint M. A proposed currency system for academic peer review payments using the blockchain technology[J]. Publications, 2017, 5(03): 19. DOI: 10.3390/publications5030019.
- [58]Sharma P. Block-VN: A distributed blockchain based vehicular network architecture in smart city[J]. Journal of Information Processing Systems, 2017, 13(01): 184-195.
- [59]Dorri A, Kanhere S S, Jurdak R, et al. Blockchain for IoT security and privacy: The case study of a smart home[C]//International Conference on Pervasive Computing and Communications. Kona, HI, USA, IEEE, 2017. DOI: 10.1109/PERCOMW.2017.7917634.
- [60]Sutherland W J, Barnard P, Broad S, et al. A 2017 horizon scan of emerging issues for global conservation and biological diversity[J]. Trends in Ecology & Evolution, 2017, 32(01): 31-40.
- [61]Shermin V. Disrupting governance with blockchains and smart contracts[J]. Strategic Change, 2017, 26(05): 499-509.
- [62]Croman K, Decker C, Eyal I, et al. On scaling decentralized blockchains[C]//Clark J. Lecture Notes in Computer Science, Christ Church, Barbados. Springer, 2016: 106-125.
- [63]Karamé G. On the security and scalability of bitcoin's blockchain[C]. 23rd ACM Conference on Computer and Communications Security, Vienna, Austria, 2016: 1861-1862.
- [64]Cocco L, Marchesi M. Modeling and simulation of the economics of mining in the bitcoin market[J]. Plos One, 2016, 11(10). DOI: 10.1371/journal.pone.0164603.
- [65]Spagnuolo M, Maggi F, Zanero S, et al. Bitlodine: Extracting intelligence from the bitcoin network[C]//Christin N, SafaviNaini R. Lecture Notes in Computer Science, Barbados. Springer, 2014: 457-468.
- [66]Li X, Wang C A. The technology and economic determinants of cryptocurrency exchange rates: The case of bitcoin[J]. Decision Support Systems, 2017, 95: 49-60.
- [67]Herian R. Blockchain and the (re)imagining of trusts jurisprudence[J]. Strategic Change, 2017, 26(05): 453-460.
- [68]Kiviat T I. Beyond bitcoin: Issues in regulating blockchain transactions[J]. Duke Law Journal, 2015, 65(03): 569-608.
- [69]Redshaw T. Bitcoin beyond ambivalence: Popular rationalization and Feenberg's technical politics[J]. Thesis Eleven, 2017, 138(01): 46-64.

## 作者简介:

程晨(1993—),女,华中科技大学公共管理学院博士研究生,研究方向为电子政务、区块链技术。

张毅(1973—),男,华中科技大学公共管理学院副院长,教授,博士研究生导师,研究方向为电子政务、智慧城市、区块链技术。

宁晓静(1993—),女,华中科技大学公共管理学院硕士研究生,研究方向为电子政务、区块链技术。

杨奕(1993—),男,华中科技大学公共管理学院博士研究生,研究方向为电子政务、大数据技术。