

美英两国区块链发展现状及对我国的启示

中国科学技术信息研究所 北京 100038

高芳

摘要 2008年以来基于区块链技术的比特币迅速在全球扩张,与此同时因具有数据唯一、去中心化和安全可信等特征,区块链技术在更广泛领域的应用前景日益显现。为了抢占发展先机,以美国、英国等为代表的国家对区块链技术及其应用给予高度关注并加紧部署。本文阐述了区块链的基本特征及典型应用,梳理了美英两国推动区块链发展的举措,在正确把握区块链技术基本特征、围绕典型应用突破关键核心技术、坚持发展和监管兼顾、推动在公共服务领域示范应用等方面得到几点启示。

关键词: 区块链, 比特币, 美国, 英国

中图分类号: G35

The Latest Development of BlockChain in the USA and the Britain and its Implications to China

Institute of Scientific and Technical Information of China, Beijing 100038, China

GAO Fang

Abstract The Bitcoin has been expanding rapidly and globally since 2008 and it is realized base on the blockchain. The key advantages of blockchain include unchangeableness data, decentralization and security, and thus it is suitable for other applications widely. For getting first-mover advantage, the United States and the Britain are stepping up the deployment of blockchain. In this paper, we described the basic characteristics and some typical applications of the blockchain, and summarized the initiatives to promote the blockchain of the United States and Britain. Some suggestions were also put forward such like profoundly understanding the essential qualities of blockchain, breaking through key technologies based on typical applications, making a balance between supervision and innovation, promoting demonstration applications in public services, etc.

基金项目: 本文受科学技术部科技创新战略研究专项(ZLY2015153)、北京市科技计划软科学研究(Z161100002816015)的资助。

作者简介: 高芳(1980-), 副研究员, 工学博士, 情报学博士后, 研究方向: 科技政策、重点科技领域信息分析。

Keywords: Blockchain, bitcoin, United States, Britain

目前,区块链技术成为全球创新领域最受关注的话题之一。英国《经济学人》将区块链比喻为“信任的机器”,并做出“区块链将重新定义世界”的判断,麦肯锡将区块链技术定义为“继蒸汽机、电力、信息和互联网科技之后,目前最有潜力触发第五轮颠覆性革命浪潮的核心技术”。自2013年以来,以美国、英国等为代表的国家均对区块链技术及其应用给予高度关注,在支持技术研发、加强治理监管以及推动政府内部示范应用等维度都在加紧部署。本文简述了区块链的定义、基本特征及典型应用,梳理了美国鼓励比特币发展以及布局区块链技术的系列举措,从国家层面的区块链相关战略部署和区块链技术应用推进等维度对英国的情况进行了总结,最后得到几点启示。

1 区块链定义及特征

区块链本质上是一种由各种技术和通信协议组成的、具有普适性的互联网底层软件基础架构。在区块链的架构中,所有的数据区块按时间顺序以链条的方式组合成特定数据结构,数据块中的数据由分布式节点共识算法生成,且以密码学方式保证其不可篡改和不可伪造。由此,区块链具有数据唯一、去中心化和安全可靠等特征^[1]。

数据唯一是指区块链上存储的信息不可更改,区块链采用带有时间戳的链式区块结构存储数据,时间戳的意义在于表示数据是某个时

间写入的,从而构成一个不可篡改、不可伪造的数据库。同时数据唯一也表现在运行过程中保持链条的唯一性,不出现分叉(不会在不同的空间维度出现数据副本),而这是通过共识机制来保证的。

去中心化是指系统内的交易验证、数据存储、信息维护和传输等过程全部是基于分布式结构,即分布式记账、存储和传播,同时分布式节点之间的信任关系是通过算法而不是中心机构来建立。其中分布式记账将会计(记账)责任分散化,由整个网络的所有参与者共同记录完成;分布式存储即数据库中的所有数据均存储于所有的电脑节点中并实时更新;分布式传播指的是每一笔新交易的信息由单个节点,通过点对点(P2P)通信协议直接发送给全网其他所有的节点。

安全可信是指区块链上的信息都是采用密码学原理对数据进行加密,同时借助各节点通过共识机制等形成的强大算力来抵御外部攻击(全网共识的公开账本数据),因而具有较高的安全性。简单来说,如果攻击者想要篡改区块链账本,意味着攻击者必须拥有超过全网50%的算力才能实现。

2 区块链的典型应用

区块链技术最广泛、最成功的运用是以比特币为代表的数字货币。本质上,比特币是由分布式网络系统生成的数字货币,其发行过程

不依赖特定的中心化机构，而是依赖于分布式网络节点共同通过共识机制完成比特币交易的验证与记录^[1]。统计数据显示^[2]，目前全球比特币供应量已超 1600 万枚（上限为 2100 万枚），总市值超过 170 亿美元（2017 年 2 月 19 日，1053 美元/枚）。包括比特币在内，全球 722 种数字加密货币的总市值超过 200 亿美元^[3]（2017 年 2 月 21 日），比特币、以太币和瑞波币位列前三，其中比特币市值约占 86%。

区块链技术虽然最初是伴随比特币的设计而出现的，但之后区块链技术自身价值日益显现，特别是区块链支持创建高级的智能合约（可编程性），这使得其应用领域和范畴逐步拓展。首先，区块链技术在金融领域的应用无疑是最可直接获取的，包括跨境支付、银行结算、证券交易以及基于互联网的股权众筹等。其次，区块链的公开透明、安全性、唯一性以及可追溯性等特征，使其天然满足数据公证和审计等的需求。在数据存储利用方面，区块链可以实现建立在数据隐私保护基础上的数据共享和开发利用，因此也可用在特别需要对个人健康数据进行妥善存储和应用的智慧医疗领域。在资产管理方面，区块链技术既可以对知识产权、商业积分等无形资产，又可以结合物联网技术对房屋、汽车等有形资产实现确权、授权等操作。

3 美国鼓励比特币发展并加快布局区块链技术

美国政府在承认比特币合法地位的同时认识到区块链技术的发展潜力，一方面加强应用监管，另一方面与企业紧密合作谋求多方面的

研究和探索。奥巴马政府对区块链，尤其是关于区块链对美国经济潜在影响高度关注。早在 2015 年 10 月，奥巴马政府和私人公司结成伙伴关系，目标是面向执法机构开展关于数字货币和比特币的培训，对抗将数字货币用于非法用途。美国总统科技顾问委员会专门与区块链银行联盟 R3 进行沟通，特别关注区块链技术对经济各方面的影响。2016 年 9 月，美国众议院通过一项支持区块链技术和数字货币的决议^[4]。2017 年 2 月，美国国会专门成立由两党成员组成的区块链核心小组^[5]，负责围绕区块链技术和数字货币完善相关的公共政策。

关于比特币以及其他类似的数字货币，美国政府的不同部门看法各异，其中美国参议院国土安全及政府事务委员会在 2013 年底公开承认比特币的合法性，认为比特币是合法的金融服务。美国国家税务局（IRS）则将比特币看做一种财产，而不是一种货币，2014 年 3 月发通知对比特币交易活动征税。美国商品期货交易委员会（CFTC）于 2015 年 9 月将比特币和其他数字密码货币定义为大宗商品。

从 2015 年起美国开始重视对数字货币的监管，然而实际的监管进程并不顺利。2015 年 6 月，纽约金融服务部门（NYDFS）发布最终版本的数字密码货币公司监管框架 BitLicense。2015 年 11 月，美国证券交易委员会（美国联邦证券监管机构）针对围绕区块链技术和分布式账本技术的炒作发出警告——区块链技术的应用可能会增加金融系统中的信任度，但目前仍处于起步阶段，监管机构、学术界以及资本市场参与者都要对其进行持续性评估，特别是监管机构要发挥引导作用，在挖掘其应用潜力

的同时要积极应对不确定性所带来的挑战。一直到2016年6月,在BitLicense的监管框架下,纽约州成功获得许可的企业只有2家(成功申请的数量为22家),与此同时包括加利福尼亚州、康乃迪克州、乔治亚州、新罕布什尔州等在内的美国其他州也未能顺利制定并实施相关监管政策^[6]。

在加快布局区块链技术方面,除了美国央行之外,美国国土安全部支持用于国土安全分析的区块链应用研究^[7],美国国防部高级研究计划局(DAPPA)则支持区块链用于保护高度敏感数据方面的探索,以及区块链在军用卫星、核武器等数个场景中的应用潜力^[8],美国电信巨头AT&T已开发出将区块链用于服务器的技术,并部署相关专利布局^[9]。

4 英国将区块链列入国家战略部署

英国将发展分布式账本及区块链提升到国家战略高度,并由财政部、数字经济部两部门共同主导推进。与此同时,在金融交易以及财政经费使用等领域,相关部门正积极推动探索性应用。

2016年1月,英国政府首席科学顾问Mark Walport发布专题研究报告《分布式账本:超越区块链》^[10],认为支撑分布式账本技术的算法是一种强大的、具有颠覆性影响的创新,它将变革公共与私营服务供给方式,并可有效提高生产力。报告将“分布式账本”定义成一个可以在多个站点、不同地理位置或者多个机构组成的网络里进行分享的资产数据库。该网络的全体参与者都可以获得一个唯一的、真实账本

的副本,同时账本内的任何改动都会所有的副本中被反映出来。账本内存储的资产可以是金融资产、实物资产和电子资产,基于密码学确保这些资产的安全性和准确性。根据共识机制,账本中的记录可以由某个、部分或者全体参与者共同更新。报告同时明确区块链是支撑分布式账本的底层技术。

报告围绕愿景、技术、治理、安全隐私、信任互联以及政府内潜在应用等维度为英国发展分布式账本提出8条建议。

(1) 愿景。政府支持分布式账本技术开发的首要目的是改善自身业务流程从而提升公共服务质量和水平,因此要在适当的范围内部署实施这项技术,并支持包括大型骨干企业、成长型以及新兴企业的创新型应用。

建议1:建立部长级工作机制,确保在政府内提供实施分布式账本技术的平台;出台顶层战略规划和发展路线图,并持续评估其他建议、跟踪领域动态,抢占先机,强调在此过程中政产学研要紧密合作,必要时建立临时的顾问专家组。

(2) 技术。分布式账本技术仍处于发展初期,其中区块链支撑分布式账本技术迈出了最重要的一步。分布式账本技术可以有“无需许可”(比如比特币)和“基于许可”两种模式,政府则更应侧重后一种模式,即只有有限的人群甚至是个人具备更改账本的权利。

建议2:围绕分布式账本的可扩展性、安全性及其内容的准确性等问题,要加大研发投入,并确保高性能、低延迟特性以及高能效。

建议3:支持地方政府创建分布式账本示范项目,集聚所有要素完成测试推动其应用。

(3) 治理。有效的治理和监管是分布式账本成功实施的关键,这需要在分布式账本系统参与者利益和社会更广泛利益之间取得平衡,同时要防治监管框架过于严格从而阻碍创新。

建议 4: 政府要设立分布式账本技术监管框架,同时随着分布式账本技术部署和应用的发展,监管框架及其实施也要同步发展。技术规范和法律条款都是实现政府监管的有效手段。

(4) 安全与隐私。虽然分布式账本有很强的抵御网络攻击的能力,但硬件漏洞和软件缺陷仍可能造成安全性和保密性风险。

建议 5: 政府需要与学术界、产业界合作,确保为分布式账本及其内容的完整性、安全性和隐私保护制定标准,这些标准同样要在监管规则和软件代码里同步反映出来。

(5) 信任与互联。为了最大程度地发挥分布式账本的作用,应确保分布式账本与其他账本的互联,这不仅包括验证机制上的互联,也更需要数据和政策的互联,同时在国际标准的有效实施方面达成共识。

建议 6: 政府需要与学术界、产业界合作,要面向个人和机构提供最高效实用的身份认证、授权协议,并与国际标准的实施建立紧密关联。

(6) 面向政府的潜在应用。政府承担多种职责,其中诸如价值分配、监管实施等活动会因为分布式账本的应用得到改进或增强。

建议 7: 理解分布式账本的真正潜能需要对其进行研究并在实践中应用,政府应积极实施分布式账本技术的测试案例,以评估该技术在公共部门的可用性。同时这些测试成果应及时用作建议 1 中路线图的控制依据。

建议 8: 除了自上而下的领导和协调外,

还应创建一个跨部门机构,以开发潜在的应用,并在行政部门内建立完善相应的知识与技术体系。同时政府作为分布式账本技术的积极使用者,还承担着引导商业部门去探索和应用分布式账本技术的职能。

在区块链技术具体应用层面,2016 年 2 月,英国金融市场行为监管局(FCA, Financial Conduct Authority)明确表示将为区块链技术发展提供一定的空间,因此不会对其进行管制^[11]。2016 年 3 月,英国央行与伦敦大学合作,开发央行控制的数字货币 RSCoin^[12],其目的不仅仅在于开发受央行控制的数字货币本身,而是为央行未来部署数字货币奠定框架性基础。2017 年 2 月,FCA 批准伦敦当地的区块链初创公司 Tramonex 登记成立小型电子货币机构(EMI)^[13],允许其在国内有效发行基于区块链的货币,这是区块链技术公司从 FCA 获得 EMI 授权的首例。除了在数字货币应用领域,英国政府也在积极探索区块链技术在其他领域的应用,比如追踪公共资金的使用,对学生贷款申请归还流程进行跟踪,用比特币发放科研经费以了解科研支出的使用情况。

5 对中国的启示

综上所述,区块链技术的去中心化信用、不可篡改和可编程等特点,使其在数字加密货币、金融交易、数据公证、数据存储、资产管理等领域有着广泛的应用前景,并有望在优化现有经济运行效率、促进行业间跨界融合等层面面对未来经济社会发展产生重大影响。由此,以美国、英国等为代表的发达国家纷纷发力,

一方面强化区块链技术在金融服务领域的监管,另一方面也在积极布局区块链技术在其他特定领域的研究和应用等。在中国,作为国家最高的货币金融管理组织机构,中国人民银行积极探索区块链技术在数字法定货币领域的应用^[14,15],贵阳市政府给出了区块链技术在政务、民生、商务发展应用的总体设计蓝图^[16]。借鉴美英两国发展区块链的部署举措,结合中国区块链技术及应用现状,得到以下几点启示:

首先,客观深刻理解区块链技术基本特征,高度重视其对未来经济社会的影响。一是正确理解去中心化特征,去中心化是一个相对的概念,完全的去中心化是系统所有参与者都拥有“更改”数据的权利,部分的去中心化即只支持有限人群“更改”数据,实际应用过程中要根据具体需求对完全去中心化和部分去中心化进行选择,这对于需要进行管控的应用领域尤其重要。二是正确理解区块链与互联网的关系,作为互联网底层架构的内嵌技术,区块链实现的是基于数据互联和信息传递基础上的信任互联和价值传递,这意味着所有与互联网相关联的领域都有望基于区块链技术实现优化升级。

其次,围绕典型应用场景突破区块链关键核心技术。目前区块链技术仍处于早期发展阶段,在众多领域还只停留在验证性应用阶段,为抢占这一新兴领域发展主动权,应加快突破区块链关键核心技术,特别是结合具体应用才能更好的解决特定场景下的隐私保护、安全性、性能扩展等问题。比如,在金融服务、能源互联网等领域,加快部署区块链应用的技术难点、业务场景、风险管理、行业标准等方面的研究。

再次,平衡好发展和监管之间的关系。一

方面要加强安全监管防范系统性风险。加强区块链应用相关的法律问题研究,加快完善优化相关法律法规,将区块链技术纳入合理合规的监管框架内。另一方面要避免监管不当可能导致的阻碍创新发展的问题,在实践中需要根据具体情况实时调整监管框架。

最后,积极探索区块链技术在政府内部以及公共服务领域的应用。充分挖掘区块链技术的安全可信特性,推动实现部门内和部门间的数据互通,实现政务信息共享和高效利用,同时推进区块链在福利发放、土地所有确权登记、医疗保险等公共服务领域的试点示范。此外,政府与产业界、学术界要紧密合作,密切跟踪全球区块链技术的发展并加强发展趋势的客观预测。

参考文献

- [1] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.
- [2] Blockchain Monitoring Website [EB/OL]. [2017-02-08]. <https://blockchain.info>.
- [3] Cryptocurrency Monitoring Website[EB/OL]. [2017-02-21]. <http://coinmarketcap.com/>.
- [4] Higgins S. Blockchain Support Bill Passes Vote in US Congress[EB/OL]. [2017-02-01]. <http://www.coindesk.com/blockchain-support-bill-passes-us-congress-vote/>.
- [5] Congress Gets Serious about Blockchains[EB/OL]. [2017-02-15]. <http://polis.house.gov/news/documentsingle.aspx?DocumentID=398291>.
- [6] Reese F. A Slow Awakening: 2016 in US Blockchain Policy[EB/OL]. [2017-02-21]. <http://www.coindesk.com/a-slow-awakening-2016-in-us-blockchain-policy/>.

[7] Higgins S. US Government Awards \$600k in Grants for Blockchain Projects[EB/OL]. [2017-02-11]. <http://www.coindesk.com/us-government-grants-blockchain-projects/>.

[8] Wong J I. Even the US Military is Looking at Blockchain Technology to Secure Nuclear Weapons[EB/OL]. [2017-02-12]. <https://qz.com/801640/darpa-blockchain-a-blockchain-from-guardtime-is-being-verified-by-galois-under-a-government-contract/>.

[9] Higgins S. AT&T is Seeking a Patent for a Bitcoin-Powered Server[EB/OL]. [2017-02-01]. <http://www.coindesk.com/att-seeks-patent-bitcoin-powered-server/>.

[10] Government Office for Science. Distributed Ledger Technology: Beyond Blockchain[R]. London, Government Office for Science, 2016.

[11] Palmer D. UK Financial Regulator Vows to Give Blockchain 'Space' to Grow[EB/OL]. [2017-02-01].

<http://www.coindesk.com/uk-financial-regulator-blockchain-space-grow/>.

[12] Bank of England. Bank of England Working on Bitcoin Alternative RSCoin[EB/OL]. [2017-02-01]. <https://www.itnews.com.au/news/bank-of-england-working-on-bitcoin-alternative-rscoin-416779>.

[13] Young J. UK Government Grants Permission to Issue Blockchain-Based Currency[EB/OL]. [2017-02-12] <https://cointelegraph.com/news/uk-government-grants-permission-to-issue-blockchain-based-currency>.

[14] 姚前. 中国法定数字货币原型构想[J]. 中国金融, 2016(17):13-15.

[15] 徐忠, 姚前. 数字票据交易平台初步方案[J]. 中国金融, 2016(17): 31-33.

[16] 贵阳市人民政府新闻办公室. 贵阳区块链发展和应用[R]. 贵阳, 2016.