区块链金融：创新、风险及其法律规制

崔志伟*

内容摘要：区块链的技术创新主要表现为分布式记账、非对称性加密及智能合约等，在金融领域的价值主要是能够助推数据信息共享、提高价值传输效率、增强信息安全和可信度、实现征信科学化，以及防范合同诈骗、票据诈骗及贷款类犯罪的发生。但其去中心化会对金融监管造成挑战，价值传输的匿名性也会助长洗钱、恐怖资助、涉外汇、网络敲诈等犯罪，增加取证、侦查的难度。对于虚拟货币和区块链不宜采取相同的监管政策，区块链金融需要在沙箱式监管下实现创新，监管部门主导完成风险的跟踪测试。金融监管的必需性决定了完全去中心化的公有链不宜适用于金融领域。对金融区块链的法律监管宜采取平台监管与业务监管并行模式，对于前者需要加强对平台运营资质及用户准入的身份审核，对于后者需要根据从事的业务功能划分监管权属。

关键词：区块链金融　去中心化　价值传输　法律监管

中国分类号：D913　　**文献标识码**：A　　**文章编号**：1674-4039-(2019)03-0087-98

DOI:10.19404/j.cnki.dffx.20190307.011

一、引　　言

近些年来，比特币等虚拟货币及其所依托的区块链技术日益为人们所知悉，当国人热衷于数字货币的“投资”时，政府突然叫停。2017年9月，中国人民银行等七部门联合下发了《关于防范代币发行融资风险的公告》，将各类代币发行业务定性为“非法”，随后中国互联网金融协会发布了《关于防范变相ICO活动的风险提示》，一时间比特币价格大跳水，国内首家比特币交易所“比特币中国”关闭所有交易功能，仅剩基于区块链技术所固有的“挖矿”业务。〔1〕对于比特币等虚拟货币的法律规制，各国的态度并不一致，积极探索者有之，完全禁止者有之，但法规主要限于加密货币和ICO，世界各国政府基本都认识到其背后的区块链技术的价值。〔2〕即便当下的这种数字货币不存在，其他立足于同样底

* 华东政法大学法律学院博士研究生、德国奥斯纳布吕克大学访问学者。

本文系上海市085工程“华东政法大学博士生海外访学资金专项资助”阶段性研究成果。

〔1〕参见刘慎良、程婕：《比特币中国昨日中午关闭数字资产和人民币充值功能 国内比特币平台将继续“挖矿”》，《北京青年报》2017年9月28日，第A16版。

〔2〕“Blockchain regulation: Technology is welcomed, cryptocurrency regulated”，https://www.intellectsoft.net/blog/blockchain-government-regulation，July 17, 2018.

层程序和分布式记账技术的方案也会产生和发展。[3]就此而言,“链圈”与“币圈”并不等同,随着区块链 1.0 向 2.0 甚至 3.0 的发展,对于区块链的价值探讨不应再局限于虚拟货币层面,而应着力实现区块链本身的技术价值与社会各行业的对接。世界经济论坛调查显示,到 2027 年,全球 10 %的 GDP 将会通过区块链技术存储,[4]在金融与科技融合不可逆转的大形势下,更是有人认为区块链技术与金融的结合使金融行业进入“区块链 +”时代。[5]在 2015 年的 Money20/20 会议上,美国第一资本金融公司的一份调查显示,将近 20%的参会者认为,区块链技术将在未来 3—5 年内对金融业产生巨大影响,超过了物联网(17%) 和人工智能(9%) 。[6]但是,区块链技术在金融领域的创新发展不可避免地会与金融监管发生冲突,法律规制便成为一个无法逾越的议题。显然,对于区块链技术不宜像代币发行那样“一刀切”,但其可能引发金融风险甚至刑事犯罪也是一个客观事实,从法律角度探讨规制限度和方式就显得尤为必要。

二、区块链的技术创新及其在金融领域的价值

金融市场发展至今不断推陈出新,从线下资本交易到互联网金融模式,银行等金融机构对社会资金的绝对控制地位日益受到冲击,一些互联网融资平台的出现给资本分配带来便利的同时,也由于监管不到位引发了诸多的金融风险。这些融资平台实际上充当着类金融机构的角色,在资金转移上仍旧存在一个“中心化”的问题,区块链技术的存在则是对这种模式的彻底变革。简而言之,区块链是一种加密的分布式记账技术,其中“加密”是一个密码学概念,“分布式”是一个互联网概念,“记账”则是一个金融概念。这种价值传输模式是数字化和分散式的,其交易信息包含在具有密码保护的各区块中,并由被称为节点的匿名用户所共享。区块链不断增长,所谓的已完成区块是最近的交易,每个匿名交易都带有时间戳,以此(借用哈希算法) 链接到下一个区块。[7]具体而言,则主要包含了以下技术。

(一) 分布式记账技术

区块链一改过去权威金融机构中心化记账模式,其交易信息(账本) 由每个参与者(节点) 共同维护,每个节点都可以保存全部加密交易数据的完整副本。每项交易数据在加入分布式账簿之前,都要向全部节点宣布且需经过多数节点(51%) 的验证和核实(即区块确认) ,交易一旦入账(即记入区块) 就不可删除、撤销或修改。网络节点持续地监控和接收分布式账簿的状态,从而确保一致性,避免记录被篡改。由于全网每个节点都掌握了全部交易数据,用户之间凭借公开、共享的信息认知便可建立信任,无须第三方的记录和证明来确认信息的准确性。[8]相较传统的中心化信任机制,这种分布式记账技术的优点主要体现在三个方面。

其一,能够真正实现信息共享、对称。以资金借贷为例,“传统的直接融资和通过金融机构的间接融资具有很大的信息不对称性,即借贷双方很难广泛了解彼此的资金去向需求,于是资金借贷在很

〔3〕“CPMI report on digital currencies”, https://www.bis.org/cpmi/publ/d137.htm, July 17, 2018.

〔4〕Roman Korizky: “World Economic Forum Survey: 10% of global GDP may be stored with blockchain technology by 2027”, http://www.coinfox.info/news/3184-world-economic-forum-survey-10-of-global-gdp-may-be-stored-with-blockchain-technology-by-2027, July 17, 2018.

〔5〕周梅丽、顾陈杰、黎敏:《区块链金融法律问题研究》,《金融纵横》2017 年第 8 期,第 69 页。

〔6〕Pete Rizzo, “Capital One Survey Finds Blockchain Interest Growing at Money20/20”, https://www.coindesk.com/capital-one-blockchain-impact-financial-services/, July 18, 2018.

〔7〕“21 experts tell us what the future looks like for cryptocurrencies and blockchain”, https://www.focus-economics.com/blog/cryptocurrencies-block-chain-future, July 18, 2018.

〔8〕李长银、李虹含、高寒、陈涛:《区块链技术的发展趋势及其对金融业的影响》,《海南金融》2017 年第 2 期,第 32 页。

大程度上限于熟人社会关系”,[9]闲散资金有效利用率低。互联网融资模式的出现虽然能够通过信息平台的居间介绍很大程度上降低这种不对称,有效实现资金的供需对接,但作为中心化的融资平台还是掌握着绝对的信息优势。如果该平台刻意积蓄(资金池)甚至挪用资金,出借方难以察觉。如果实现了“区块链+融资”,资金的去向便是透明、共享的,每个参与借贷的用户通过区块链记载的数据,能够处于同等地位、互相监督,不存在绝对的信息优势或者信息垄断。据有关统计,截至2015年,我国P2P网络借贷行业共有1302家企业倒闭、668家平台“跑路”,其中,最大一家平台“跑路”导致风险暴露资金额达到46亿元人民币,对社会稳定造成了负面影响。[10]其中不乏涉嫌非法吸收公众存款甚至集资诈骗犯罪。究其原因,主要是由于这种互联网融资模式并未完全实现去中心化,投资者对网络信贷的信任主要是对平台的信任,[11]但又缺乏对中心平台的有效监管,导致中心化的信任机制难以真正确立。并且,即便是在传统的权威金融机构内部,中心化的绝对信息优势也为从业人员违法违规提供了便利。譬如新近报道的“储户近千万元资金被支行行长擅自转出,用于偿还其个人高利贷”事件。[12]这显然并非个案。在信息不对称、不透明的情形下,储蓄方的违约成本便大大降低,带来的是储户的资金风险与从业人员违法犯罪风险的升高。在区块链技术运用下,储户对于资金的动向可以有着形象的认知,以此对金融机构形成有效监督,另外,监管者也完全可以作为区块链的一个节点与参与者共享数据信息,以此最大程度减少监管的视觉盲区。

其二,传统的中心化交易模式跨度长、成本高,国际支付更是如此。以支付宝为例,虽然这种第三方支付方式的运用解决了电商交易中的信任难题从而带来了交易的极大便利,但资金交易、变现过程中多节点、流程长也是一个客观事实,如果交易双方支付宝绑定的银行账户不同,更是如此。这种多节点导致的高成本在跨境支付上表现得便十分明显。在资金汇入(汇出)行与其代理行(清算行)不属于同一家银行的情况下,受制于SWIFT报文转换、行号严要求以及时差导致的运行时间等因素,人民币跨境支付的效率大打折扣。[13]如果是外汇支付,经过当地行、中央银行、境外银行等一系列转移程序,外汇交易费、当地行汇费以及对方行手续费等也使交易成本大大提高。区块链技术的运用便可以将这些节点直接串联起来,能够缩短时间跨度、降低交易成本。例如,建立在比特币区块链基础上的瑞波(Ripple)协议,尝试建立一个点对点的跨境支付系统,在这种模式下每一个银行都成为区块链的一个节点。[14]瑞波(Ripple)系统里的货币兑换(包括各国的“法定货币”以及虚拟货币)和交易的效率更高、速度更快,且交易费用几乎为零,交易确认在几秒钟内完成,没有异地和跨行费用。[15]分布式记账省却了银行间的授信、核查等流程,由先前的“多点共治”转为“线型传输”,提高了交易效率。再如,在传统证券交易中,证券所有人发出交易指令后,指令需要依次经过证券经纪人、资产托管人、中央银行和中央登记机构这四大机构的协调,从证券所有人处发出交易指令,到交易最终在登记机构得到确认,通常需要“T+3”天才能完成交易,多节点导致时间跨度拉长。使用区块链,买卖双方能够通过智能合约直接实现自动配对,并通过分布式的数字化登记系统,自动实现结算和清算。[16]由此可见,区块链的分布式记账技术可以将先前的“多节点”并入一个链条当中,实现参与主体的直接对接,能够大大提高价值传输的效率。

其三,分布式记账技术将数据信息进行N多备份,各个节点同步更新,增加了篡改的难度、减少

〔9〕崔志伟:《互联网融资的法律风险与规制——以P2P网贷平台为分析视角》,《金融教育研究》2015年第6期,第35页。

〔10〕张荣:《区块链金融:结构分析与前景展望》,《南方金融》2017年第2期,第63页。

〔11〕郑迎飞、陈晓静、罗龙文:《中国P2P网贷的信任模型及实证研究》,《上海对外经贸大学学报》2017年第3期,第41页。

〔12〕孔令晗:《储户千万巨款遭银行“内鬼”转出自用》,《北京青年报》2018年6月30日,第A08版。

〔13〕参见王雪、陈平:《人民币跨境结算模式的比较与选择》,《上海金融》2013年第9期,第46页。

〔14〕参见前引〔5〕,周梅丽等文,第70—71页。

〔15〕[加]唐塔普斯科特、[加]亚力克斯·塔普斯科特:《区块链革命——比特币底层技术如何改变货币、商业和世界》,凯尔、孙铭、周沁园译,中信出版社2016年版,序言。

〔16〕秦谊:《区块链冲击全球金融业》,《当代金融家》2016年第2期,第43页。

了出错的概率。在原有的信息集中化处理的中心模式下，操作者的一点点失误便可能关系全局，甚至也不排除工作人员在他人不知不觉中对系统信息进行篡改的可能。在分布式记账模式下，每个参与者均是系统信息的维护者和受益者，对信息删改的难度大大增加。因为，账簿中每条信息的变动均需经过 51%以上节点的确认，否则修改无效。除非操作者掌握了足够的算力，否则难以取得大部分的认可。并且，区块链中的每一区块虽然链接在前一区块之上，但并非传递式分布，即后一区块的信息存储并不以前一区块为转移（新区块一旦生成即包含了前一区块的所有信息），即便是成功对某一区块信息进行删改，也不影响整个链条的运作。这无疑增强了信息安全和可信度，真正实现交易透明化、自主化。

通过以上分析可见，分布式记账技术带来的是共识机制的改变，即“去中心化”或“去信任”技术，网络上的价值传输模式被改变，不再依赖于传统的可信任的第三方或者中心机构。〔17〕

（二）非对称性加密算法和时间戳

在信息传递中，保密是保证信息有效性和真实性的重要方式，加密技术便是通过某种技术手段把直白的重要的信息变为乱码（加密）后传送，对方收到信息后再用相同或不同的手段还原（解密）。密码学是区块链的关键组成部分，〔18〕区块链上的价值传输需要保证参与者签名的不可复制性、与信息内容的一一对应以及对签名的身份鉴别，传统意义上的手写签名显然无法做到这点。这种数字签名通过密码学哈希算法以及非对称加密技术共同实现。首先，区块链采用密码学哈希算法技术（SHA-256），保证区块链账本的完整性不被破坏。这种哈希函数计算对输入内容具有极强的敏感性，信息内容发生任何的微小变化，所得出的哈希值便发生非常大的变动，〔19〕以此保证了数字签名与信息内容的绝对对应。其次，哈希算法属于一种公开函数，每个人借此得出的计算结果（哈希值）会完全相同，数字签名的可鉴别性需要非对称加密技术的介入。这种非对称加密不同于加密解密互为逆向操作的对称性加密，安全性更高，加密与解密采用私钥和公钥两种不同的密钥。其中私钥具有私密性、专属性、唯一性，私钥持有者即为本人；公钥则具有公开性、非专属性，通过私钥加密的信息只有通过公钥才能解密，反之亦然。交易主体通过私钥对交易信息的哈希值进行加密，将此加密数据连同公钥一并发送给潜在的合作方，合作方运用收到的公钥对加密数据进行解密，将解密后的哈希值与原始信息的哈希值进行比对，如果两者完全一致，则能确保此交易信息未被篡改、系该交易主体的真实意志体现。否则，该交易信息便不足采信。通过这种密码技术，最大程度保证了数据传输的真实性，未（经中心机构撮合）建立起信任的个体便可基此达成稳定共识。

这种密码学数字签名技术的运用很大程度上提高了交易的安全性、可信性。尤其在金融领域，信用是安全的保证，通过伪造数字签名或印章而进行交易欺骗的技术难度大大增加，违法犯罪的风险随之降低。

在商务往来中，文件签署的时间与签名同样重要，“需要在经过数字签名的交易上打上一个可信赖的时间戳，从而解决一系列的实际和法律问题”。〔20〕“时间戳可以作为区块数据的存在性证明，有助于形成不可篡改和不可伪造的区块链数据库，从而为区块链应用于公证、知识产权注册等时间敏感的领域奠定了基础。”〔21〕因为，交易信息一旦加盖时间戳后，就具有不可逆性，且使每笔交易数据均可追本溯源、逐笔验证。〔22〕这为交易争端中的责任确认无疑提供了很大的技术支持。除此之外，加盖时间戳即确保了交易的唯一性，防止行为人在同一时间或短时间内“一物多卖”。例如在票据支付中，“通过时间戳可以完整地反映票据从产生到消亡的全过程，具有不可篡改、不可伪造和可追溯的特

〔17〕Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, July 18, 2018.

〔18〕Jorn van Zwanenburg, “What Is Cryptography?”, https://www.investinblockchain.com/what-is-cryptography/, July 18, 2018.

〔19〕参见《华为区块链白皮书》，2018 年 4 月，第 11 页。

〔20〕张科伟、唐晓波：《带有时间戳的安全电子交易协议》，《计算机应用研究》2004 年第 9 期，第 169 页。

〔21〕袁勇、王飞跃：《区块链技术发展现状与展望》，《自动化学报》2016 年第 4 期，第 485 页。

〔22〕参见林晓轩：《区块链技术在金融业的应用》，《中国金融》2016 年第 8 期，第 17 页。

性”，能够有效防止伪造票据、一票多卖等违法犯罪现象的发生。〔23〕

（三）智能合约

智能合约不同于传统意义上的手写合同，它利用软件技术来自动完成一项交易，只要各方具备了先前设置的各种条件。它也不是民法意义上的合同，而是一种智能软件，只要满足预定条件，就可以控制或记录甚至产生特定的法律相关活动。〔24〕作为一种嵌入式程序化合约，计算机专家将各方事先协商确定的权利义务事项通过计算机的程序语言转换为代码并设计算法，计入区块链当中，只要条件成熟便自动执行，无须第三方的督促，也不会发生合同对方拒不履行现象，从权利义务设定、签署到执行实现了一体化，具有数据透明、不可篡改、永久运行等特性。〔25〕可编程特性使得参与方可以增加任意复杂的条款，技术因素的介入减少了人为参与，自然便使履约成本降低，全程的可视化、自动化也能够保证合约内容的高准确性。并且，监管者只需对交易者商定的权利义务内容进行合法性审查，即可一举完成对整个交易过程的监督，也就可以降低监管成本。

在金融领域，尤其是涉及大宗资金的证券交易以及票据中，智能合约的运用不仅可以降低出错概率以及违约风险，还能通过对合约中行业交易规则的细化规避欺诈、操纵等明显违法行为。除此之外，结算清算的一体化、自动化也能够省却既往的人为节点，从而控制交易成本。2016 年高盛发表的一份报告指出，区块链技术每年可为股票市场节省高达 60 亿美元的资金。〔26〕这是因为，“区块链可以创建一个开放式、防篡改的交易总账，它可能取代并简化证券交易中许多复杂的系统”，在这种金融脱媒模式下，“买方和卖方能够通过智能合约直接实现自动配对，并通过分布式的数字化登记系统，自动实现清算和结算”，〔27〕并且结算具有了实时性，几乎就在交易完成的瞬间完成结算工作。

对于金融从业者而言，最大的执业风险莫过于刑事风险，而对于投资者或交易者，最大的损失也是刑事犯罪带来的经济损害。以上所述三个方面的区块链技术能够增加某些犯罪的实施难度，从而起到抑制犯罪的作用。例如，对于合同诈骗罪，由于合约变为自动执行，履行合同过程中实施诈骗的可能性空间就得到很大程度压缩；由于票据信息实现区块联动、实时更新，伪造、变造或者使用作废票据的技术难度增大；数字签名的严格对应性及可识别性，使通过伪造印章、签名来签订合同的难度也增加。除此之外，对于区块节点（用户）过往交易的综合分析也能够基本判断其实际履行合同的能力。这种分析模式类似于比特币交易中的输入值与输出值比对以确定行为人是否具备支付能力，并且可以将此模式广泛适用于银行等金融机构征信系统。以往的征信模式主要由金融机构自主收集、分析用户的信用记录、进行信用等级评定，但这种传统模式可能存在失察、片面等弊端，并且人工审查的难度较大。〔28〕如在贷款业务中，依靠工作人员对贷款申请材料的真伪以及申请人的信用进行审核往往消耗过多的人力资源，且工作人员一旦存在或故意或过失的审查错误，便会导致银行的信贷资金陷入无法追回的风险。区块链技术在银行借贷方面的运用，既可以增加申请人伪造信息的难度，也可以对申请人既往的借贷情况以及其公司或个人收支情况进行核算，将可预期的收入

〔23〕任安军：《运用区块链改造我国票据市场的思考》，《南方金融》2016 年第 3 期，第 40 页。

〔24〕“Blockchain and smart contracts”，https://www.pwc.de/en/newsletter/it-security-news-en/blockchain-and-smart-contracts.html，last visit on August 12, 2018.

〔25〕参见工业和信息化部信息中心：《2018 年中国区块链产业白皮书》，第 99—102 页。

〔26〕Goldman Sachs: “Blockchain tech Could Save Capital Markets $6 Billion a Year”，https://www.coindesk.com/goldman-sachs-blockchain-tech-save-capital-markets-12-billion/，July 12, 2018.

〔27〕李利军：注意了，区块链来得或许远比你想像的要快！，载搜狐财经网 http://www.sohu.com/a/73599849_324659，2019 年 1 月 15 日。

〔28〕其实，这也是传统的线下信息征集模式的普遍局限。例如，在社会公众参与中，传统的公众纸质投票、人工计票方式，人工成本高且计票差错难以避免，而在“互联网+公众投票”下，能够记录整个投票过程，数据实时存档有利于对投票活动的监督，为后期的票数分析提供了全面记录。林艺、马祺：《“互联网+公众投票”：法治公信的新场域》，《云南大学学报（社会科学版）》2017 年第 1 期，第 113 页。区块链模式则是在互联网科技基础上的进一步升级，为公众提供更宽的参与渠道且能够增加整个参与过程的透明度，使公众真切感知到自身参与的实际效果。

作为“输入值”，将借贷资金作为“输出值”，确保其具备实际的还款能力。并且，在区块链模式下，金融机构也可以对行为人的资金去向进行监督，以此降低骗取贷款、高利转贷甚至贷款诈骗的刑事风险。既然资金链条透明可见、可溯查，在个人融资中，行为人擅自将资金改变用途的难度就增大，以此可抑制互联网融资中非法集资类犯罪的发生。这种区块链模式也可用于公司内部的财务管理，财务信息不再由某特定人掌控，而是由管理层共享、共治，个人挪用、侵吞公司财产的空间就能得到有效压缩。当社会进步到能够以技术杜绝某些犯罪现象或者使这种可能性降到极低，也就可以节省诸多的司法资源。

三、区块链金融所蕴含的技术风险与法律风险

（一）初始阶段的技术薄弱可能引致的风险

区块链 2.0 毕竟处于初始阶段，技术研发尚不完备，因此，在区块链金融发展的前期，可能会由于技术“漏洞”而引发一些金融难题。首先，“从目前的情况来看，区块链的性能问题主要表现为吞吐量和存储带宽的能力远不能满足整个社会的支付需求……比特币交易结算每秒钟可完成 7 笔到 10 笔，但坦率来说，这个速度是银行难以接受的，更是广大客户所无法承受的”。〔29〕如果应用于大频次、大资金的证券交易场，更是形成了对其性能的严重挑战。这是因为，交易记录的生成需要大多数节点进行区块确认，这就意味着节点基数越大，就需要多达成一次共识，确认所需的时点就越长。尤其对于向用户完全开放的公有链来说，虽然节点越多便意味着非法行为者依靠强势算力进而篡改数据的难度就越大，系统的安全性和公平性也就越高，但节点的增多同时也意味着效率的相应下降，节点数和效率就成为了一个悖论。〔30〕就此而言，区块链技术的研发尚需解决安全与效率如何兼得的难题。其次，虽然相较传统交易模式，区块链所采用的密码学技术能够增强系统的安全性，但也并非无懈可击，“随着计算能力的不断进步，这些机制的基本弱点更加难以消除。例如，量子计算机能够破解性能最强的普通电脑难以破解的加密算法”。〔31〕一旦密码被破解，交易信息乃至数字签名均有被篡改的可能。最后，由于区块确认遵循少数服从多数的原则，一旦不法行为人掌握了足够（51%以上）的挖矿能力（算力），便能够成功篡改和伪造区块链数据。这主要会发生在两种情形下：某一区块链处于起步阶段，节点较少，控制当然就相对容易；虽然节点多，区块链系统较为完善，但高利诱惑还是让不法行为人不惜挑战高难度技术。“Bitcoin Gold 受黑客攻击案”就是后一情形，攻击者部署大量服务器通过“51%的攻击”控制 Bitcoin Gold 超过一半的网络哈希率，虽然发动此类攻击的成本高、难度大，但黑客最终从中牟利 1800 万美元。〔32〕由此可见，区块链研发者还需在技术层面不断攻坚。这种技术本身引发的风险是创新过程中的“试错”机制所容许的，随着研究的不断深入，势必能够对症下药、弥补技术漏洞。因此，这种风险是无须过于戒惧的，只是在金融领域，未经风险测试前不宜全面铺开。

（二）去中心化导致的监管难题以及异化的风险

如上所述，分布式记账技术依靠节点的共同参与来维护交易信息，不再依靠中心化机构的权威性来取得信任，区块链金融一旦实现，势必会对现今的政府（或其授权的）管理部门的地位以及现行法规构成挑战。譬如，在公司股权登记领域，按照《公司法》的规定，有限责任公司应该向公司登记机关办理登记，未经登记不得对抗第三人（《物权法》对于机动车登记也有着类似的规定），这主要是基于登记机关的公信力。但在区块链系统中办理股权转让，“公司股权的登记及其变动的公信力不再依

〔29〕张歆：《监管应跟随区块链技术演进同步加强》，《证券日报》2018 年 4 月 28 日，第 B2 版。

〔30〕参见公有链——区块链产业底层平台主流模式，载链门户网 http://www.lianmenhu.com/blockchain-2648-2，2018 年 7 月 24 日。

〔31〕[美]凯文·沃巴赫：《信任，但需要验证：论区块链为何需要法律》，林少伟译，《东方法学》2018 年第 4 期，第 96 页。

〔32〕黑客使用 51%算力攻击热门比特币交易所，牟利 1800 万美元，https://www.secrss.com/articles/2981，2018 年 7 月 10 日。

靠第三方来提供而是依靠全体参与者来共同维护”,“区块链账本更具不可篡改性和极高的公信力,甚至让为了对抗第三人而需在工商局登记股权信息的行为变得多余”。[33]在技术的催动下,私权自治变得更加彻底。在监管方式上,由于传统的中心化模式有了技术优势作为替补,这种去中心化在某些方面引发了纯粹技术性措施无法实现的监管难题。

典型的数字加密货币依赖于分布式记账技术的使用,该技术提供了一种新方法来保留所有权记录并将所有权从一个用户转移到另一个用户,通常几乎没有关于所有者身份的信息。

在区块链中,每个参与节点的身份并非是真名实姓,而是一串数字代码。例如,比特币依赖于区块链,区块链由全世界通过匿名交易分类账链接在一起的匿名计算机运行。数字货币通过计算机处理能力、互联网技术以及密码学来实现自动化,以便将价值从一个人转移到另一个人。该技术的维护,安全性和可靠性由分散的开发者社区处理,这通常缺乏强有力的治理。正是因此,一些加密货币似乎很容易受到洗钱的影响。由于许多加密货币在其分类账中很少或根本没有关于加密货币所有者身份的信息,因此该工具的持有人通常被认为是其所有者。[34]也就是说,在区块链价值传输中,基于隐私权保护的要求,人们更关注的是交易的实际内容,而对交易内容与参与者真实身份的关联性可能会缺乏关注,这就会造成冒用他人身份或者使用虚假身份从事不法行为的现象。例如,在“李某冒用他人身份洗钱”一案中,犯罪嫌疑人李某在诈骗某公司得手后,试图将诈骗所得货币“洗白”。于是,在网上购买了张某、王某两个人的身份证复印件及与其名字对应的一套银行卡和电话卡,李某利用他人信息在某比特币交易平台注册账户后,即以网名“微风”的名义与平台客服联系,要求充值。客服发现充值数额较大,遂要求“微风”发送身份证正反面照片。李某以照片的形式发给客服一张王某身份证复印件,客服只核对了身份证复印件与注册时信息相符,没有进一步确认此笔业务的操作人与注册客户是否为同一人的前提下,即同意充值 200 万元。以此,李某成功洗钱 200 万元。[35]一些犯罪分子也正是利用了这种真实身份与实际交易的弱关联性,以虚拟货币为中介实施犯罪。虚拟货币的可匿名以及可现金交易的特征,往往导致身份溯源之难题。这种对比特币的滥用可能会助长黑色市场交易、逃税、洗钱以及恐怖组织资助。[36]我国《刑法》关于洗钱罪规定了五种行为方式:提供资金账户;协助将财产转换为现金、金融票据、有价证券;通过转账或者其他结算方式协助资金转移;协助将资金汇往境外;其他掩饰隐瞒行为。比特币等虚拟货币的出现可以为以上各种行为方式提供便利,如为行为人提供比特币账户、协助将赃款转换为比特币、通过以比特币为中介的方式将资金转往境外等。由此看来,虚拟货币的放开与反洗钱的监管措施应当同步,否则势必会被不法分子所利用。

实施网络敲诈的犯罪分子也往往会利用比特币的匿名特征,例如一些黑客攻击他人计算机或加密他人文件,以此威胁用户向某比特币账户发送“赎金”。并且这种方式不限于线上,如向餐饮店发送敲诈信要求支付特定数量的比特币,“正是利用了比特币的匿名性特征,不法分子‘完美’避开了监管部门通过银行卡交易记录追踪每笔钱来龙去脉的可能”。[37]也正是因此,全球极端组织正在讨论把比特币作为购买武器以及获得资金援助的一种手段。[38]除此之外,如果放开虚拟货币市场,基于区块链的国际一体化,这种货币便可在国际间自由流通,甚至可以在越过央行监管的情形下,直接转换为外币。也就是说,将人民币转换为外币不再需要央行的审核,可以通过先以人民币购买虚拟货币,再通

〔33〕杨东、潘曌东:《区块链带来金融与法律优化》,《中国金融》2016 年第 8 期,第 26 页。

〔34〕Lael Brainard,“Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?”https://www.federalreserve.gov/newsevents/speech/brainard20180515a.htm, July 23, 2018.

〔35〕肖飒、张超:《反洗钱义务下区块链数字货币平台的民事责任》,《证券时报》2016 年 8 月 13 日,第 A04 版。

〔36〕Trevor I. Kiviat,“Beyond Bitcoin:Issues in Regulating Blockchain Transactions”,Duke Law Journal,Vol.65:589.

〔37〕赵丽:“玩家”揭露利用比特币洗钱内幕:国内买国外卖,载中国新闻网 http://www.chinanews.com/cj/2017/05-17/8225929.shtml,2018 年 7 月 10 日。

〔38〕比特币可能带来恐怖融资风险,载币行网 https://www.okcoin.cn/shequ/themeview.do?tid=1014194,2018 年 7 月 10 日。

过匿名交易汇往境外，最后再转换为外币。这种行为虽然有骗购外汇罪的实质，[39]但在调查取证上无疑具有相当的难度。再如，许多贪腐分子之所以青睐于现金，正是基于查证上的困难。比特币盛行之后，不排除会出现以比特币行贿再提现或者先收取现金再购买比特币等现象，从而增加了贿赂犯罪的侦破难度。

以上所述是区块链或虚拟货币本身所蕴含的法律风险，目前来说，区块链的运行机理对于普通公众而言还是一个陌生概念，在比特币高投资潜力的衬托和渲染下，以 ICO 为方式，以区块链业务为名而行违法犯罪之实的现象也日益加剧。这虽然与区块链本身没有关联（毕竟技术是中立的），但确实也是市场规则的缺失给了非法者可趁之机。这主要表现为“传销币”和“空气币”两种。前者如“李某暗黑币案件”，被告人李某在香港创办某科技公司，创建虚假的虚拟货币“暗黑币”投资，借助真正暗黑币的名声及价值进行宣传，其实无任何实体经营活动，以高额返利为诱饵，由全国各个地区的负责人及会员通过宣传、上课、介绍等方式不断发展下线。[40]后者如深圳普银集团有限公司发行的“普银币”，通过恶意操纵价格以及还本付息承诺的方式诱骗他人投资。[41]所有这些“项目”均是打着区块链和虚拟货币的名义蹭热度，对公众的财产安全造成极大的威胁。就此而言，在监管措施尚不健全的情况下，国家“一刀切”制止代币发行是有其合理依据的。

四、“区块链 + 金融”：法律监管的双层模式

（一）法律介入区块链金融的原则和尺度

正是基于区块链多方面的技术创新及其良好的应用前景，以及“区块链不等于币圈”这一事实，[42]对于虚拟货币和区块链不宜采取相同的监管政策，国家虽然原则上禁止了虚拟货币的发行，但不能直接推导出对区块链也是排斥的。正如在欧洲议会和欧洲委员会联合主办的“区块链聚焦”研讨会上 MEP Jakob von Weizsäcker 所主张的：“现阶段干预可能为时尚早，因为我们作为立法者尚未充分清楚地知道主要问题是什么，所以为了不扼杀创新，我们不希望它现在就成为现实。”[43]也正是因此，英国、美国、新加坡等国家采取了沙箱监管来应对金融领域的创新。其核心理念在于确保适当的安全措施已经到位的同时，允许企业在真实的市场环境下对创新的产品、服务和商业模式进行风险测试。[44]其旨在不产生重大风险的情况下推进金融包容性的创新，监管沙箱由监管机构建立，允许初创公司和其他创新者在监管机构的监督下在受控环境中进行实时实验。[45]直言之，监管沙箱就是一块试验田，监管者为之提供真实的市场环境。虽然不予干预但一直处于监控之下，如果能够排除系统性风险方能允许市场普及，否则予以清退，由此实现了监管与创新的平衡。

沙箱模式完全可以运用到区块链金融当中，为实现最大的消费者权益保护，需要在监管者的密切“监视”下实现金融创新，在最终得出测验结果之前监管者不应以强力介入或禁止，但这并不代表金融创新无需监管。通过限制性监管来鼓励金融科技的创新，这才是“沙箱”精神，因此，区块链金融

〔39〕参见谢杰：《区块链技术背景下金融刑法的风险与应对——以比特币交易对外汇犯罪刑法规制的冲击为视角》，《人民检察》2017 年第 8 期，第 63—66 页。

〔40〕肖飒：揭开“区块链”为名的非法传销伪装，载亚洲财经网 http://www.asiafinance.cn/zjzl/101505.jhtml，2018 年 7 月 15 日。

〔41〕参见克己：《“普银币”骗局：以区块链为幌子行非法集资之实》，《国际金融报》2018 年 5 月 21 日，第 07 版。

〔42〕郭钇杉：《区块链不等于币圈 关键看应用的场景》，《中华工商时报》2018 年 4 月 4 日，第 01 版。

〔43〕Noelle Acheson, “Regulating Ethereum? EU Parliament Weighs Blockchain´s Big Issues”, https://www.coindesk.com/regulating-ethereum-eu-parliament-weighs-blockchains-big-issues/, July 21, 2018.

〔44〕FCA: “Regulatory sandbox lessons learned report”, https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf, July 21, 2018.

〔45〕Ivo Jenik, “Regulatory Sandboxes: Potential for Financial Inclusion?”, http://www.cgap.org/blog/regulatory-sandboxes-potential-financial-inclusion, last visit on July 21, 2018.

这种价值互联网也确实需要密切监控。[46]上海市《互联网金融从业机构区块链技术应用自律规则》(以下简称《自律规则》)对此便有所体现,该规则第4条规定,互联网金融从业机构的区块链技术应用在面向社会前应当通过具备相关资质的第三方测试和评估,并由律师事务所出具独立法律意见书;同时应当客观、及时、准确地进行相关信息披露,不做虚假、夸大及误导性宣传。第6条规定,应用区块链技术必须通过相关风控与合规部门进行风险管控与合规评估,严格遵守监管部门的相关要求。

现有的区块链分为公有链、联盟链和私有链三种,从"去中心"的程度来看,三者分别是完全去中心化、弱中心化以及强中心化,监管的难度自然是公有链最大、联盟链次之、私有链最易。[47]在笔者看来,联盟链最适合运用到金融领域。其一,完全的去中心化在金融领域并不现实。金融的高风险性以及公众利益的密切关涉性决定了不可能缺乏监管,但"由于没有中心系统,很难锁定客户的多个匿名账户,除非掌握秘钥,否则很难了解资金去向,这极可能被犯罪分子利用"。[48]其次,"公有链的各个节点可以自由加入和退出网络,并参加链上数据的读写",在准入资格上缺乏审核,而"联盟链的各个节点通常有与之对应的实体机构组织,通过授权后才能加入与退出网络",[49]也就是说,"联盟链相对于公有链非常重要的特点就是节点准入控制与国家安全标准支持,确保认证准入、制定监管规则符合监管要求,在可信安全的基础上提高交易速度"。[50]就此而言,公有链在监管上过于粗犷,高度的开放性使金融监管难以实现。完全的去中心化虽然有助于高效率的实现,但难以获得安全保证。[51]再次,发展区块链技术需秉持其设计初衷。出于对纸币发行体系的不信任,中本聪提出并创造了基于区块链技术的去中心化的虚拟货币"比特币",试图规避"央行—纸币"这一现代金融体系的内在不稳定性。但发展至今,比特币不仅呈现出极度的不稳定性,还给不法分子开发"空气币""传销币"以可趁之机,[52]这不得不让人们反思区块链技术的初衷,并非一味地为去中心化而去中心化,而是最大限度规避金融风险、实现、保护参与者利益。最后,上文已述,币圈与链圈应秉持不同的监管原则,公有链虽然适用于比特币、以太坊等虚拟货币,但区块链金融毕竟不同于区块链数字货币,从有效监管的角度讲,这不宜照搬到金融领域。

综上所述,区块链金融需要在沙箱式监管下实现创新,监管部门主导完成风险的跟踪测试。金融监管的必需性决定了完全去中心化的公有链不宜适用于金融领域,该领域应淡化"去中心化",强调分布式、弱中心特征,[53]因此联盟链更为适合。这其实是区块链分布式共治优势与中心化有效性监管优势的中和。对于金融安全目标的实现,第三方"看门人"的角色不可或缺。[54]在权威监测下确保金融创新的实现,正是沙箱经验的体现。

(二)法律监管的应然模式和具体措施

我国的金融管理体制长期适用"机构监管",即将金融机构类型作为划分监管权限的依据,同一类型的金融机构均由特定的监管者监管。[55]但随着诸多新型金融产品的出现,这种监管体制面临着

〔46〕"Regulation vs. Innovation in the Internet of Value", http://bitlegal.io/2016/06/20/the-internet-of-value-is-innovation-a-by-product-of-proactive-regulation-or-does-innovation-always-come-first/, July 21, 2018.

〔47〕但是私有链的强中心化与传统的监管模式无异,不能充分发挥区块链的优势,可以适用于部门内部,但不适合整个金融领域。

〔48〕王硕:《区块链技术在金融领域的研究现状及创新趋势分析》,《上海金融》2016年第2期,第29页。

〔49〕区块链的类型都有哪些,载搜狐网 http://www.sohu.com/a/227317183_100120800,2018年7月21日。

〔50〕前引〔25〕,工业和信息化部信息中心文,第18页。

〔51〕参见前引〔10〕,张荣文,第57—58页。

〔52〕黄金萍:比特币背叛比特币,载南方周末 http://www.infzm.com/content/122273,2019年1月15日。

〔53〕杨涛:《区块链金融应用面临十大挑战》,《上海证券报》2016年12月13日,第12版。

〔54〕参见王超:《从区块链看金融创新与法律变革》,《检察风云》2016年第20期,第66页。

〔55〕黄韬:《我国金融市场从"机构监管"到"功能监管"的法律路径——以金融理财产品监管规则的改进为中心》,《法学》2011年第7期,第109页。

挑战。新型的金融机构可能存在着多种营业类型，以此造成监管规则多元化、政出多门的局面；并且随着一些新型领域的出现，如虚拟货币、ICO，难以确定其法律性质，也就难以划分监管职责。“功能监管”模式与此不同，可以绕过金融产品法律定性的争议，直接按照其实际“功能”来划分监管权归属。如，在美国，虽然未承认比特币等虚拟货币的“法币”地位，但美国证券交易委员会认为 ICO 中出售的许多代币具有证券的功能，因此将其纳入规制范围内。〔56〕这种模式能够很大程度上解决监管的重叠化或空白化，可以作为传统监管模式的补充。除此之外，笔者认为，我们需要对“区块链 + 金融”模式有着不同层次的理解和对待。一方面，区块链实际上是一种去中心化的数据库，是一种价值互联网，因此在平台管理上，可以沿用传统的互联网管理模式；另一方面，除数字货币外，区块链金融均是区块链技术与具体金融领域（如支付结算、票据、证券）的结合，对此，“功能相同就应归入相应分类进行监管”。〔57〕就此而言，区块链金融就形成了平台监管以及业务监管并行的双层模式。

1.平台监管：加强对平台运营资质及用户准入的身份审核

金融监管的必需性决定了并非任何主体均可作为区块链平台发起者从事金融业务，除了上述“沙箱”式风险监测外，还需加强对其资质和真实身份的审核和登记。《自律规则》第 7 条便规定，互联网金融从业机构应用区块链技术应当向当地监管部门及行业自律组织进行报备，主动接受行业监管与自律管理；报备信息至少应包括项目名称、责任人、业务模式、业务风险、风控措施等。由此，可实现对区块链业务平台的跟踪监管。同样，《美国联邦银行保密法》（Bank Secrecy Act,BSA）要求银行和其他金融机构做好各种登记和记录保存，所有货币服务业务都必须在财政部门登记以及发展出反洗钱和客户识别程序。2013 年 3 月，金融犯罪执法网络（FinCEN）将这种规则扩展到“可兑换的虚拟货币”的相关参与者，即便这种货币不具有“法币”的地位。在 FinCEN 的要求下，“交易者”和“管理者”可能会受到规制，“交易者”是指将虚拟货币兑换成真实货币、资金或其他虚拟货币的机构或个人；“管理者”是涉及发行也有权回收虚拟货币的机构或个人。2014 年 FinCEN 发布了四项规则，与既存的 BSA 一起提供了关键的监管意见。第一，任何的区块链交易均适用虚拟货币交易（的监管规则），因为，即便是非金融区块链也需要最低数额的货币，因而也需要对“交易者”和“管理者”进行类似的规制。第二，开采虚拟货币的用户（矿工）不属于货币变送者（即“交易者”和“管理者”），即便他们用比特币购买商品和服务，并且，矿工也可将虚拟货币兑换为真实货币或其他虚拟货币而不受 BSA 的规制，但这均限于个人用途，如果他们将销售比特币作为一种商业活动，则受到（如同“交易者”）规制。第三，在某些情况下挖掘比特币的矿工公司也不属于货币变送者，比如，将虚拟货币用于购买商品或服务，或支付先前发生的债务，或者用于公司自身的投资等。第四，无论公司是作为经纪人（匹配、促成交易）还是经销商（在自己账户中交易），都被视为“交易者”。〔58〕

在州一级，纽约州金融服务部一直是颁布适用于加密货币的规则的领导者。例如，2015 年 6 月，该机构为虚拟货币活动创建了第一个营业执照，称为 BitLicense。法律要求加密企业遵守反洗钱法，“了解你的客户”（“KYC”）和其他汇款规定。总而言之，传统的监控机制在加密货币领域发挥着越来越重要的作用。例如，几乎每个数字货币交换现在都要求新的注册人进行一系列的“KYC”验证步骤，并且一旦经过验证，通常情况下加密货币的购买和销售的上限相对适中。〔59〕

通过以上所述的国外经验，我们基本可以延伸出以下启示：

其一，这种监管规则可以适用于所有的区块链平台，因为，每个区块链的发起者均是在或多或少

〔56〕Marc Press/Joseph B. Doll,“Blockchain and Cryptocurrency: Recent Legal and Regulatory Developments”, https://www.cscorporate-blog.com/2018/03/articles/recent-developments/blockchain-cryptocurrency-recent-legal-regulatory-developments/, July 20, 2018.

〔57〕前引〔31〕，沃巴赫文，第 104 页。

〔58〕前引〔36〕，Trevor I. Kiviat 文，S.590—593.

〔59〕Marjorie J. Peerce/Brad Gershel,“Beyond Best Practices: Regulatory Compliance Now a Necessity in the Cryptocurrency Sector”, https://www.moneylaunderingwatchblog.com/2017/12/beyond-best-practices-regulatory-compliance-now-a-necessity-in-the-cryptocurrency-sector/#more-3349, last visit on July 20, 2018.

地变相“发行货币”（任何区块链都需要“挖矿”作为奖励机制，即便是非金融区块链也需要最低数额的“货币”），那么，发起者（即上述“管理者”）以及虚拟货币的兑换者（如果允许虚拟货币自由兑换的话）均在重点监管之列，需要将资质、平台信息以及反洗钱等合规计划向监管机构报备，不经此报备及批准，任何机构或个人不准发展区块链业务。并且，为了限制虚拟货币所导致的金融风险以及对“法币”地位的冲击，宜将支撑区块链发展的“矿金”限于比特币、以太币等几种，不宜过度扩张此范围。

其二，应严格要求平台对用户真实身份的审核职责，如《自律规则》第 8 条便规定，互联网金融从业机构应当加强客户身份识别、认证，严格遵循实名交易、“了解你的客户”等原则，并加强平台之间的互联互通；严格遵循反洗钱相关规定，对可疑交易及时发现、及时上报。即区块链节点（用户）在交易中虽然可以用密钥（公钥）作为其身份象征，但并不代表背后的真实身份信息就不重要，相反，平台应加强所加入节点的交易身份与其真实身份的审核，确保实际交易者与注册信息所显示的行为主体保持一致，并且，对于大额可疑交易，平台具有向监管部门举报的义务。2018 年欧盟理事会通过一项指令要求，虚拟货币和法定货币之间的兑换服务提供商以及钱包托管服务提供商有义务对可疑活动进行识别，当局应监视加密货币在这些平台上的使用，国家金融情报部门应有途径采集相关信息，并将这些交易地址与所有者对应起来。[60]否则，便会因此承担法律责任。如在“李某冒用他人身份洗钱”中，充值平台便会承担审核不严的法律责任。再如在 Ripple XRP 虚拟货币兑换商被处罚案中，FinCEN 对其处罚理由主要是作为货币服务机构未经注册即销售虚拟货币，以及未实施和维持足够的反洗钱（AML）计划来保护其产品不被洗钱者或恐怖分子所利用。[61]

上文已述，完全开放、进退自由的公有链并不适合金融领域，应淡化节点的“匿名”色彩，对用户准入进行实名审核。如欧盟主管机关便认为比特币等加密电子货币的匿名性正是吸引犯罪集团进行洗钱的主要管道，欧盟执委会 2016 年 2 月即发布声明表示，执委会已提案要求将虚拟货币交易平台纳入反洗钱计划的管制目标，如此一来，这些平台在将虚拟货币兑换成实体货币时就必需遵守客户尽职调查的规定，终止这类交易平台的匿名交易。实名认证的相关身份证明文件可以是护照、有效的身份证明或电费单的居住证明等。[62]

其三，可以从“数额 + 用途”的角度明确监管的重点。例如，可将用于商品和服务等个人用途的交易不列在监管之中，重点对于大额或者商务往来中的交易进行监管。除此之外，交易的频次如果异常，也应当从用户身份、交易对象、交易额、交易内容等方面进行审核。

2.业务监管：根据从事的业务功能划分监管权属

平台监管是各类业务的共同模式，此外，还需结合业务的功能进行专业监管。如果所从事的金融业务主要是虚拟货币的发行、兑换，则实际上具备了货币的功能（即便不承认其“法币”地位），则应将其纳入央行监管。例如，2015 年高盛集团、花旗银行与美国银行均提交了基于区块链技术的专利申请，具体包括“数字货币的风险监测系统”、“数字货币可疑用户警报系统”等。[63]通过这种风险监控以及平台的监管义务，可以对洗钱、逃汇等违法犯罪交易形成很大程度的遏制。如果所从事的是证券发行业务或者具有证券的实际功能（如 ICO 通过公开发售筹集资金，可以在二级市场上出售），则可以纳入证券交易所的监管。例如，2015 年美国纳斯达克证交所和 Chain 合作推出了私人企业股权交易

〔60〕欧盟：更新反洗钱法案以解决与虚拟货币相关的风险问题，http://www.8btc.com/eu-adopts-rules-to-reduce-anonymity-for-crypto-users-2，2018 年 7 月 21 日。

〔61〕P.H.Madore,“Ripple Labs Fined $700,000 by FinCEN for Non-Compliance”，https://www.cen.com/ripple-labs-fined-700000-fin-cen-non-compliance/，July 20, 2018.

〔62〕林国宾：阻断恐怖组织金援欧将严管比特币，载中时电子报 http://www.chinatimes.com/cn/newspapers/20160503000067-260203，2018 年 7 月 24 日。

〔63〕杨东：金融的革命就该有科技的手段，载中国科技网 http://www.stdaily.com/zhuanti01/kjcxbrt/2016-12/19/content_486609.shtml，2018 年 7 月 24 日。

平台 Linq，用于处理私人证券市场的股票交易。〔64〕

总而言之，平台监管与业务监管并行不失为一种可选的监管模式，其中平台监管是各金融业务类型的共同前提和基础，业务监管则是在此基础上进一步的监管细化。

结　语

区块链的技术运用至金融领域将会是继互联网金融之后又一个金融创新，这种加密的分布式记账方式很大程度上能够克服传统中心化记账高成本、高人为风险等弊端，对预防一些违法犯罪也甚有助益。但完全的去中心化不宜照搬到金融领域，安全与效益之间，在技术难以保证两者可兼得的情况下，应当优先选择前者，就此，金融监管始终不可缺位，弱中心化的联盟链是金融领域的最优选择。监管上，除了需加强对平台资质的审核、用户信息的登记以及业务模式的分类管辖外，还需注意到两点：其一，区块链应用的跨国界性质需要全球性的监管协调，〔65〕传统的自治模式显然就不合时宜，就此，积极借鉴国外经验展开国际合作就非常必要；其二，节点的匿名化固不可取，需要对平台及用户的身份信息进行审核，但如何加强对合法隐私的技术和监管保护值得进一步探究。

Abstract: The technological innovation of block chain is mainly manifested in distributed ledger technology, asymmetric encryption and smart contracts, etc., its value in the financial field is mainly to promote data information sharing, improve the efficiency of value transmission, enhance information security and credibility, and achieve scientific credit reporting, and to prevent contract fraud, bill fraud and loan crimes. But its decentralization will challenge financial supervision, the anonymity of value transmission will also contribute to crimes such as money laundering, terrorist financing, foreign exchange, network extortion, and increase the difficulty of forensics and investigation. For virtual currency and block chain, it is not appropriate to adopt the same regulatory policy, block chain finance needs to be innovated in a regulatory sandbox where the regulatory authorities take the lead to complete the risk tracking test. The necessity of financial supervision determines that the completely decentralized public chain is not suitable for the financial field. The parallel mode of platform supervision and business supervision should be adopted in the legal supervision of financial block chain. With regard to platform supervision it is necessary to strengthen the identity audit of platform operation qualification and user access, for business supervision, we need to divide the ownership of supervision according to the business function.

Key words: block chain finance, decentralization, value transmission, legal supervision

〔64〕参见前引〔33〕，杨东等文，第 25 页。

〔65〕黄锐：《金融区块链技术的监管研究》，《学术论坛》2016 年第 10 期，第 56 页。