信任，但需要验证：论区块链为何需要法律

[美]凯文·沃巴赫（Kevin Werbach） 著*
林少伟 译**

内容摘要：区块链是一项具有变革性的基础技术，其对世界的潜在影响堪比互联网。本质上来讲，区块链和法律都是信任机制，两者关系的不确定性引致对区块链两极分化的评价。区块链利用分布式分类账、共识和智能合约等特征实现避免对中央机关的依赖以及建立普遍诚信的价值主张。但区块链信任系统并非无懈可击，分类账、智能合约、边缘服务提供商以及代币销售各层次各有风险，网络解放和政府架空无异于天方夜谭，法律和监管介入的需求毋庸置疑。监管可能抑制创新并引起管辖权竞争问题，但并非无解之局。区块链可以补充法律、与之互补甚至取而代之，两者分别有其治理局限性，融合治理方为解决之道，而这可以通过法律代码化与代码法律化两种模式实现。

关键词：区块链 比特币 智能合约 法律代码化 法律监管

区块链可谓是互联网问世后信息技术领域最重要的发展。为比特币等数字货币提供支持是区块链的设立初衷，但事实上，区块链的作用远不止此：其还为解决人际间由来已久的信任问题提供了新思路。古语有云，“矩不正，不可为方；规不正，不可为圆”。纵使区块链潜力无穷，若无有效管理，其对增进信任毫无助益。由于与法律实施完全脱节，区块链系统可能会起反作用，甚至造成危险后果。其与法律的关系也并非表面看来那样疏离。问题的焦点不在于如何监管区块链，而在于如何利用区块链进行监管。区块链可以补充法律、与之互补甚至取而代之。过度或不成熟地适用严格的法律义务都会阻碍创新，拒绝利用技术达成公共政策目标的机会。区块链开发者和法律机构可以携手共进，但必须承认对彼此的独特作用。

一、引言：代码的逆袭

区块链[1]被称为是“最有可能改变未来十年商业模式的技术”，[2]同时也被称为犯罪活动、[3]庞氏

* 美国宾夕法尼亚大学沃顿商学院法律研究和商业道德副教授。
感谢 Dan Hunter 对本文观点形成的贡献，感谢 Sarah Light、Patrick Murck 以及 2017 年 Lastowka Cyberlaw 研讨会和 2016 TPRC 会议的与会者对本文早期初稿所提出的宝贵意见。
** 西南政法大学民商法学院副教授、人工智能法律研究院区块链研究中心主任。
本文是“西南政法大学人工智能法律研究教师研究创新项目资助”阶段性研究成果。

骗局、[4]无政府[5]和独裁主义[6]的避风港。这样两极分化的评价源于区块链与法律关系的不确定性。区块链技术的拥护者认为其是克服地域法律制度缺点的民主化方法。批评者则认为这是规避法律责任的高招。这两种观点谈不上孰对孰错。两者都过分关注区块链的监管问题,却忽视了区块链本身的监管作用。为扬长避短,区块链系统需要与法律实施和制度相结合。

2009 年,以比特币加密货币[7]为基础,中本聪提出了区块链概念,迅速在全球传播开来。自 2016 年年末到 2017 年年中,比特币的价格暴涨 10 倍,加密货币的总市值超过 1200 亿美元。[8]2013 年到 2016 年,风险投资者向区块链初创公司注入超过 10 亿美元的资金。[9]2017 年,区块链项目本身数量也创历史新高,通过向用户和投资者直接销售代币,募集到超过 20 亿美元[10]的资金。

区块链技术的浪潮不仅席卷到创业型企业,科技巨头(例如 IBM、微软和英特尔)以及主要专业服务公司(例如普华永道(PWC)和毕马威(KPMG)[11])也开始向区块链领域进军。[12]世界上最大的金融机构几乎都在依照相同原则直接或共同使用分布式分类账技术,[13]政府也不例外。有些在试验分布式分类账平台,而各国央行(例如英格兰银行和中国人民银行)则在探索独立发行加密货币的可行性。[14]冷静如高盛集团的观察者,也看到这一"唾手可得的"机遇背后数十亿美元的年收益。[15]虽然区块链近期的爆红可能名不副实,但长远来看,其极有可能成为价值交换的分布式基础。[16]

〔1〕"区块链"一词在术语使用上尚未达成共识。从技术层面来说,区块链(或称"区块链条")是一种利用了有序标记的区块的信息储存系统,此点将于本文第二部分详述。正如"互联网"一样,"区块链"一词或能描绘出其乾坤,公共区块链的子集,或者仅为比特币的公共分布式账簿。但让人更加困惑的是,有些"区块链"平台既不使用区块链条,也不使用像比特币一样的数字货币。描述这类系统更加准确的术语是分布式分类账技术(DLT)。

〔2〕*See* Don Tapscott and Alex Tapscott, *The Impact of the Blockchain Goes Beyond Financial Services*, HARV. BUS. REV. (May 10, 2016). https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services.

〔3〕*See* Kim Zetter, *FBI Fears Bitcoin's Popularity with Criminals*, WIRED . COM (May 9,2012,10:51pm), https://www.wired.com/2012/05/fbi-fears-bitcoin/.

〔4〕*See* Matt O'Brien, *Bitcoin isn't the Future of Money – it's Either a Ponzi Scheme or a Pyramid Scheme*, WASHINGTON POST WONKBLOG(June 8, 2015),http://www.washingtonpost.com/blogs/wonkblog/wp/2015/06/08/bitcoin-isnt-the-future-of-money-its-either-a-ponzi-scheme-or-a-pyramid-scheme/.

〔5〕*See* Matthew Sparkes, The Coming Digital Anarchy, Telegraph (June 9, 2014, 2:25pmBST), http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html.

〔6〕*See* Ian Bogost, *Cryptocurrency Might be a Path to Authoritarianism*, A TLANTIC (May 30, 2017), https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/.

〔7〕加密货币是数字货币的形式之一,它通过密码学的方法而非国家或金融机构的支持来获得保护。*See* Part II(A), infra.

〔8〕*See Buoyant Bitcoin Stirs Crypto-Bubble Fears*, REUTERS (Aug. 10, 2017, 7:18am EDT),https://www.nytimes.com/reuters/2017/08/10/business/10reuters-markets-currencies-crypto-analysis.html.

〔9〕Garrick Hileman, *State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin*, COIN DESK (May 11, 2016, 15:15 BST), http://www.coindesk.com/state-of-blockchain-q1-2016/.

〔10〕*See Tech Start-Ups Raise $1.3bn This Year From Initial Coin Offerings*, FINANCIAL TIMES (July 18, 2017), https://www.ft.com/content/1a164d6c-6b12-11e7-bfeb-33fe0c5b7eaa?mhq5j=e1. N.B. need updated cite reflecting the $2 billion number.

〔11〕*See Jeff John Roberts, Can IBM Really Make a Business Out of Blockchain?*, FORTUNE ,June 28, 2016, http://fortune.com/2016/06/28/ibm-blockchain/; Anna Irrera, Microsoft Unveils Technology to Speed Up Blockchain and Its Adoption, REUTERS (Aug. 10, 2017, 9:10am),https://www.reuters.com/article/us-microsoft-blockchain-idUSKBN1AQ1KD.

〔12〕*See Blockchain Services*, PWC, https://www.pwc.com/us/en/financial-services/fintech/blockchain.html.

〔13〕*See Nathaniel Popper, Envisioning Bitcoin's Technology at the Heart of Global Finance*, N.Y. TIMES DEAL BOOK BLOG (Aug. 12, 2016).http://www.nytimes.com/2016/08/13/business/dealbook/bitcoin-blockchain-banking-finance.html ("该报告估计,全球80%的银行可能会在明年之前启动分布式分类账本项目").

〔14〕*See Chuan Tian, China's Central Bank Opens New Digital Currency Research Institute*, COIN DESK (June 30, 2017, 10:00 UTC), https://www.coindesk.com/chinas-central-bank-opens-new-digital-currency-research-institute/; John Barrdear and Michael Kumhof, The Macroeconomics of Central Bank Issued Digital Currencies, Bank of England Staff Working Paper No. 605 (July 2016),http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf.

〔15〕*See James Schneider et al, Blockchain: Putting Theory into Practice*, GOLDMAN SACHS EQUITY RESEARCH REPORT (May 24, 2016), https://www.scribd.com/doc/313839001/Profiles-in-Innovation-May-24-2016-1.

〔16〕*See Marco Iansiti & Karim R. Lakhani, The Truth About Blockchain*, HARV. BUS. REV. Jan./Feb. 2017 (将区块链作为"基础性技术"的巨大潜力进行了描述,但仍需要时间才能充分实现).

区块链是一项复杂的技术,但其基本功能非常简单,即提供分布式但高度精准的记录。换言之,每个个体都可以保留一份自动更新的分类帐副本,但这些副本都保持不变,即使没有中央管理员或原本。〔17〕这一方式有两大优势:其一,使用者可以对交易完全放心,无须受制于任何个体、中介或政府的诚信。其二,单一的分布式分类账取代需要对账的私人分类账,降低了交易成本。以数字加密技术和博弈论激励机制为基础的软件使得欺骗系统难如登天,这是达成以上目的的关键。

区块链最初的利益来源于比特币这一脱离地域性政府管控的私人数字货币。为解决欺诈、洗钱、资金外流、货币操纵和恐怖主义融资等问题,货币交易往往会受到严格管控。〔18〕在某些区域,即使法律并未明确禁止,政府和强大的私人利益集团同样会说服银行或者支付平台,叫停涉及赌博、著作权资料传播或泄露政府文件传播的服务。比特币似乎是一种不受上述限制约束的价值储藏手段和交易机制。对于(部分)"抗审查"货币而言,比特币可谓是一个利好消息。

另一方面,不受监管的货币极易成为违法行为、消费者滥用和金融投机的避风港。〔19〕比特币一度风评不佳。丝绸之路——早期的比特币市场(最初用于毒品和其他走私品交易)——就是最典型的例子。〔20〕2013 年,美国联邦调查局(FBI)关闭了丝绸之路,其经营者罗斯·乌尔布里奇被判处终身监禁。然而,在三年营业期间,丝绸之路经手处理了价值 950 万比特币的交易,时值约为 10 亿美元。〔21〕尽管之后的合法应用开始成倍增长,但对于罪犯而言,比特币是不是最好的馈赠尚无定论。

与此同时,区块链系统软件看似会阻碍传统法律实施,但其规则运行方式却与法律制度类似。这印证了网络法学者劳伦斯·莱西格(Lawrence Lessig)在其 1999 年出版的著作——《网络空间代码和其他法律:代码即法律》〔22〕——中提出的基本观点。20 世纪 90 年代,点对点文件共享引发著作权的变革,而网络言论自由脱离政府监控。法律学者亚伦·莱特(Aaron Wright)和普里马韦拉·德·菲利皮(Primavera de Filippi)指出,区块链"令公民创制习惯法体系变得更加容易,使其可在自身科技法律框架内,任意选择和实施自定规则"。〔23〕但所有线上群体都能不受政府管制,实施自定规则,仍旧是不现实的想法,实施难度极高。网络自由主义,终究是美梦一场。

2016 年年中的几周内,全世界约有 11000 人在一家虚拟的区块链公司购买了价值约为 1.5 亿美元的以太币,而该公司没有员工、缺少管理且并非合法存在。〔24〕The DAO(The Distributed Autonomous Organization,去中心化自治组织的简称)是一个完全由自我执行的软件(即智能合约)组成的线上众筹系统,〔25〕被誉为"经济合作的新范式……商业的数字民主化"。〔26〕自动代码运行于无中央权威的分布

〔17〕关于区块链如何实现这种矛盾结果的详细解释见本文第二部分。

〔18〕*See* U.S. Gov't Accountability Office, Gao-14-496, Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges 23 (2014); Jerry Brito &Andrea Castillo, Bitcoin: A Primer for Policymakers 14—15 (2013).

〔19〕*See* David Yermack, IS BITCOIN A REAL CURRENCY? AN ECONOMIC APPRAISAL, Nat'l Bureau of Econ. Research, No. w19747 (2013).

〔20〕*See* Joshuah Bearman, *The Rise and Fall of Silk Road: Part I*, WIRED (Apr. 2015),http://www.wired.com/2015/04/silk-road-1; Joshuah Bearman, The Rise and Fall of Silk Road: Part II, WIRED (May 2015), http://www.wired.com/2015/05/silk-road-2.

〔21〕US v. Ross William Ulbricht, Sealed Complaint (Sept. 27, 2013), available at https://www.documentcloud.org/documents/801103-172770276-ulbricht-criminal-complaint.html. 那时,比特币的总供应量只有大约 1200 万。

〔22〕LAWRENCE LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE (1999).为了涵盖例如社交媒体等新生事物,莱西格(Lessig)在 2006 年发布了本书更新后的版本。*See* LAWRENCE LESSIG, CODE VERSION 2.0 (2006).

〔23〕*See* Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (2015).

〔24〕*See* Nathaniel Popper, *A Venture Fund With Plenty of Virtual Capital, but No Capitalist*, N.Y. T IMES DEALBOOK (May 21, 2016), https://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html;Joon Ian Wong, The Price of Ether, a Bitcoin Rival, is Soaring Because of a Radical, $150 Million Experiment, Q UARTZ (May 20, 2016), https://qz.com/688194/the-price-of-ether-a-bitcoin-rival-is-soaring-because-of-a-radical-150-million-experiment/.

〔25〕*See* Christoph Jentzsch, DECENTRALIZED AUTONOMOUS ORGANIZATION TO AUTOMATE GOVERNANCE, https://download.slock.it/public/DAO/WhitePaper.pdf (describing the structure and functions of The DAO). 关于智能合约更加详细的讨论,*see* Kevin Werbach and Nico Cornell, Contracts Ex Machina, 65 D UKE L.J. ___ (forthcoming 2017); Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO . L. TECH. REV. 304 (2017).

〔26〕*See* Seth Bannon, *The Tao of "The DAO" or: How the Autonomous Corporation is Already Here*, TECH CRUNCH (May 16, 2016), https://techcrunch.com/2016/05/16/the-tao-of-the-dao-or-how-the-autonomous-corporation-is-already-here/.

式平台，取代法律、中介和人际关系成为信任的实现载体。随后，有人一夜之间窃取了该平台三分之一以上的资金。〔27〕

自此，事情开始变得有趣起来。〔28〕依照 DAO，被截留的资金完全合法。区块链无法辨识窃贼和客户。更为严重的是，区块链的记录恒定不变，这意味着无人能够阻止盗窃行为或者追回被盗资金。最后，为了追回资金，DAO 运行的区块链平台不得不一分为二。〔29〕反叛团体并不赞同这一决定，因而复制了被盗货币，而窃贼也保留了盗取的资金。〔30〕这听起来有些离奇，但却反映了未来的趋势。无论过去还是现在，被盗取的资金都是真实存在的。DAO 软件的确起到了取代法律实施和第三方中介的作用，但这也是其短板所在。DAO 软件虽有查验功能，但已不具可信度。原本应当势不可挡的区块链实际运行中却不尽人意，用户只好选择收回投资。

DAO 事件折射出更深层次的问题。区块链之所以需要法律，本质上来讲，是因为两者都是信任机制。分布式分类账技术使得参与者无须相信任何其他个体，只信系统结果即可。但信任同样意味着不确定性和脆弱性。〔31〕这也是里根总统最喜欢的俄罗斯谚语，〔32〕同时也是本文题目的一部分（“若你相信，就不会坚持查验；若坚持查验，就是不信”）〔33〕被认为毫无意义的原因。区块链虽然能够巧妙地解决查验的问题，但若想增强信任，还需法律从旁协助。

即使区块链能够完美运行，其设计、实施和使用都是由人来完成的。虽然其表现形式是客观代码，主观意图对这一系统仍有影响。区块链容易受到自私的行为、攻击和操纵的影响。其合法实践范围本质上是一个治理问题，而非计算机科学问题。区块链开发者并未充分认识到这一点，便莽撞闯入了法律学者争论了几个世纪的领域。

因此，问题的难点在于分类账与法律结合会有哪些后果。诸如合约、财产、公司以及司法实施之类的法律结构以规范的权利、期望和救济替代人际信任。但仍存在法律制度难以规制之处，而且某些情况下，法律规范反而会对信任造成损害。针对此类状况，区块链提出了巧妙的应对之法。然而，要想实现区块链的巨大潜力，就需要对密码学“枯燥代码”与法律“含糊其辞”各自的作用进行严谨的映射。〔34〕且令人意外的是，我们往往需要将两者相结合才能达到目的。即使在现阶段，许多尝试仍不成

〔27〕*See* Klint Finley, *A $50 Million Hack Just Showed that the DAO was All Too Human*, WIRED (June 18, 2016), https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/; Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. T IMES D EALBOOK (June 17, 2016), http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed -more-than-50-million-from-experimental-cybercurrency-project.html.

〔28〕一种说法将后续事件描述为“可以说是发生在你我生命中最具有哲学意义的轶事。” E.J. Spode, The Great Cryptocurrency Heist, AEON (Feb. 14, 2017), https://aeon.co/essays/trust-the-inside-story-of-the-rise-and-fall-of-ethereum.

〔29〕Michael del Castillo, *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*, COIN DESK (July 20, 2016), http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/.

〔30〕Paul Vigna, *The Great Digital-Currency Debate: 'New' Ethereum vs. Ethereum 'Classic'*, WALL ST. J. MONEYBEAT BLOG (Aug 1, 2016, 12:19 pm ET), http://blogs.wsj.com/moneybeat/2016/08/01/the-great-digital-currency-debate-new-ethereum-vs-ethereum-classic/.

〔31〕*See* Roger C. Mayer et al., *An Integrative Model of Organizational Trust*, 20 ACAD. MGMT. REV. 709 (1995); Denise M. Rousseau et al., Not So Different After All: A Cross-Discipline View of Trust, 23 ACAD. MGMT. REV. 393, 394 (1998); Helen Nissenbaum, *Will Security Enhance Trust Online, or Supplant It*," in TRUST AND DISTRUST IN ORGANIZATIONS: DILEMMAS AND APPROACHES 155, 173 (Roderick M. Kramer and Karen S. Cook, eds., 2004).

〔32〕众所周知，1987 年，里根（Reagan）在与苏联签订《中程核力量条约》的仪式上引用了这句格言。苏联领导人米哈伊尔·戈尔巴乔夫（Mikhail Gorbachev）愤怒地评论道：“你每次在会议上都会重复这点。”*See* DAVID E. H OFFMAN, THE DEAD HAND: THE UNTOLD STORY OF THE COLD WAR ARMS RACE AND ITS DANGEROUS LEGACY 295 (Doubleday 2009). 其实这句格言在俄语语境下会表现得更好，因为这两个动词不但押韵，而且源于同一词根。

〔33〕Barton Swaim, "*Trust, But Verify*": An Untrustworthy Political Phrase, Wash. Post (Mar. 11, 2016), https://www.washingtonpost.com/opinions/trust-but-verify-an-untrustworthy-political phrase/2016/03/11/da32fb08-db3b-11e5-891a-4ed04f4213e8_story.html.

〔34〕“含糊其辞”和“枯燥代码”这两个术语来自智能合约的创始人 Nick Szabo。*See* Nick Szabo, *Wet Code and Dry*, U NENUMERATED (Aug. 24, 2008), http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html.

熟。有些法律制度在运行方式上过于软件代码化,而有些区块链代码则过于法律化。

因此,将法律与区块链对立起来是不对的。人无完人,法律行为主体会犯错,软件设计师也不例外。区块链历史虽短,但屡遭重挫,DAO 只是其中之一。在业已完善的社区建立规则、规范、激励机制和技术结构〔35〕并非易事。有观点认为,法律应作相应变通,才能真正发掘区块链的潜力,反之亦然。区块链需要法律。其开发者如何连接整合中本聪的加密经济信任模式与法律实施的正式结构和体制,这一能力决定了区块链能够发挥多大作用。

笔者坚持这一观点:法律是区块链的必由之路,而非其毁灭的根源。这一领域的法学研究多关注加密货币的监管。〔36〕虽然比特币及其子体的法律处置还有许多问题亟待解决,但追根究底,最核心的问题在于区块链能否完全取代法律。答案是否定的。在第一部分进行回顾之后,本文第二部分描述了区块链的技术特征,并对其快速普及的原因加以阐释。第三部分阐述了在脱离法律实施的情况下,区块链系统可能出现的错误。第四部分描述了加密货币代码和法律的融合治理模式。第五部分进行总结。就网络层面而言,区块链的确可以称得上是商业、政府和社会的变革性技术,但前提是要与法律和谐共存。

二、区 块 链

短短几年内,比特币和区块链在科技领域引发狂热。〔37〕该领域的领军人物将之与互联网相提并

〔35〕这代表了莱西格(Lessig)模型中的四个规范要素。*See Lessig, supra note* 22.

〔36〕*See* Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271 (2015); Jerry Brito et al, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets & Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144(2015); Andres Guadamuz & Chris Marsden, *Blockchains and Bitcoin: Regulatory Response*, FIRST M ONDAY, vol. 20, no. 12 (Dec. 7, 2015), http://firstmonday.org/ojs/index.php/fm/article/view/6198/5163; Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191 (2016); Paul H. Farmer, Speculative Tech: *The Bitcoin Legal Quagmire and the Need for Legal Innovation*, 9 J. B US. & TECH. L. 85 (2014); Stephen T. Middlebrook & Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813 (2014); Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 L OY. C ONSUMER L. REV. 111 (2012); Wright & De Filippi, *supra note 23; Trevor I. Kiviat, Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 D UKE L.J.569 (2015); Ruoke Yang, *When is Bitcoin a Security Under U.S. Securities Law?*, 18 J.L. TECH . & POL' Y 99 (2013); Joshua Doguet, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119 (2013); Danton Bryans, Note, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L.J.441 (2014).

〔37〕*See, e.g*, Marc Andreesen, *Why Bitcoin Matters*, N.Y. TIMES DEALBOOK (Jan. 21, 2014,11:54 AM), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters; Reid Hoffman, *Why the Block Chain Matters*, W IRED , May 15, 2015; Amy Cortese, *Blockchain Technology Ushers in the "Internet of Value"*, Cisco (Feb. 10, 2016), https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1741667; Jerry Cuomo, *How Businesses And Governments Can Capitalize On Blockchain*, F ORBES B RAND V OICE (Mar. 17, 2016), http://www.forbes.com/sites/ibm/2016/03/17/how-businesses-and-governments-can-capitalize-on-blockchain/#4468fdb83a2c (将区块链称为"革命性的技术"); UK Government Chief Science Advisor, Distributed Ledger Technology: Beyond Block Chain(2015),https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf [以下简称分布式分类技术], at 4 ("在分布式的分类帐技术中,我们可能正在见证一种潜在的创造性潜能的爆发, 它促进了卓越的创新水平。"); UBS, Building the Trust Engine 5, https://www.ubs.com/microsites/blockchain-report/en/home/, at 5 ("像许多同行一样, 瑞银集团相信区块链是一种潜在的变革性技术……");ARVIND NARAYANAN, ETAL, BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 2 (*Princeton University Press 2016*) (Feb. 9, 2016 draft) ("乐观主义者声称比特币将从根本上改变世界各地的付款方式、经济甚至政治。"); DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION 8-9 (2016); *Popper, supra note 13* ("世界经济论坛的一份新报告预测到,虚拟货币比特币引入的这项基础技术将在全球金融体系中占据核心地位").

论，称之为彻底开放的分布式平台，可提供大量新颖完善的数字化服务。〔38〕有人认为，这一平台能够预防金融危机，〔39〕甚至“变革商业、政府和社会”。〔40〕其他人则提出，区块链预示着能够取代政府主导型制度的新型私法的产生。〔41〕对自由主义者而言，这些技术是不受主权国家控制的经济活动。对进步人士而言，区块链技术会摧毁根深蒂固的私有权力。而对于其他人而言，区块链仅仅是赚钱或解决问题的绝佳机会。

分布式分类账的绝妙之处在于，其能够确保特定活动可信无疑，无须以信任特定主体为前提。〔42〕亿万级企业家和风险投资者雷德·霍夫曼（Reid Hoffman）称之为“不信之信”。〔43〕区块链的支持者指出，使用区块链技术就意味着，代价高昂的调解机制和法律实施可以退位让贤了。他们指出，与其相信银行、法院和政府，不如通过开源式密码协议，选择信任数学和计算。

（一）区块链的运行机制

2008 年，有人化名中本聪，在网络发布了一篇题为《比特币：一种点对点式的电子现金系统》的文章，首次提出区块链这一概念。〔44〕对译码者而言，文中的许多观点和技术并不陌生，但该系统的运行方式却独具匠心。比特币是一种类似于现金的不记名票据。2009 年，中本聪所提的系统在开源式软件上运行，比特币自此正式进入流通。随后，不计其数的交易所如雨后春笋般在世界范围内全面开花，从事比特币与法定货币（例如美元或欧元）的交易。一些开发者努力优化比特币软件（最后一次得知中本聪的消息是在 2011 年），而世界各地的“矿工们”则为确保网络安全提供计算能力。自 2017 年 8 月开始，比特币的单币价值超过 3000 美元。〔45〕

比特币是第一个区块链系统。随后的几年内，各种各样不同的区块链系统不断问世。有些系统会针对特定用途进行优化，例如致力于促进金融服务提供商之间跨境货币兑换的瑞波（Ripple）。〔46〕而其他系统（例如以太坊（Ethereum）则是通用平台。〔47〕这些区块链均有可交易的加密代币〔2017 年中期，以太坊的以太币（Ether）市值超过 200 亿美元〕，主要目的是为了刺激市场活性。另一类系统被称为许可分类账，这一系统以服务私营公司、实现信息或交易的分享为宗旨，因而并不发行加密货币。最典

〔38〕*See* Cadie Thompson, *Bitcoin Transformative as the Web, Venture Capitalist Says*, CNBC (Jan. 28, 2014), http://www.cnbc.com/2014/01/28/bitcoin-transformative-as-the-web-venture-capitalist-says.html; Scott Rosenberg, *There's a Blockchain for That!*, BACKCHANNEL (Jan. 13, 2015), https://backchannel.com/how-bitcoins-blockchain-could-power-an-alternate-internet-bb501855af67#.r7ilkg7m9; Peter Spence, *Bitcoin Revolution Could be the Next Internet, Says Bank of England*, T HE TELEGRAPH (Feb. 25, 2015, 3:47pm GMT),http://www.telegraph.co.uk/finance/currency/11434904/Bitcoin-revolution-could-be-the- next-internet-says-Bank-of-England.html; Daniel Folkinshteyn, Mark Lennon & Tim Reilly, *A Tale of Twin Tech: Bitcoin and the WWW*, 10 J. STRATEGIC & INT ' L STUD . 82 (2015).

〔39〕*See Editorial Board, Bring on the Blockchain Future, BLOOMBERG VIEW* (June 6, 2016,10:05 AM EDT), http://www.bloomberg.com/view/articles/2016-06-06/bring-on-the-blockchain-future (“区块链真的会改变世界……”).

〔40〕Tapscott & Tapscott, supra note 2.更进一步来说，Skype 的联合创始人 Jaan Tallinn 认为区块链可以用来解决公众悲剧和一些人文学科面临的最大挑战。*See* Rebecca Burn-Callander, *Skype Inventor Jaan Tallinn Wants to Use Bitcoin Technology to Save the World*, T ELEGRAPH (June 20, 2016, 6:40pm), http://www.telegraph.co.uk/business/2016/06/20/skype-inventor-jaan-tallinn-wants-to-use-bitcoin-technology-to-s/.

〔41〕*See* Wright and De Filippi, supra note 23; Michael Abramowicz, Cryptocurrency-Based Law, 58 ARIZ. L. REV. 359 (2016).

〔42〕*See* Joshua Fairfield, BitProperty, 88 S. CAL. L. REV. 805, 814 (2015) (“比特币为信任问题创造了一种可操纵的解决方案—种不会导致中心化以及其他伴生风险和成本的验证方法”).

〔43〕*See* Hoffman, *supra note* 37.

〔44〕Satoshi Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System 8 (2008), https://bitcoin.org/bitcoin.pdf. 中本聪的身份从未被确凿地证实。

〔45〕Bitcoin Price Index, https://www.coindesk.com/price/.

〔46〕*See* Nathaniel Popper, *The Rush to Coin Virtual Money With Real Value*, N.Y. TIMES DEALBOOK (Nov. 11, 2013, 4:17pm), https://dealbook.nytimes.com/2013/11/11/the-rush-to-coin-virtual-money-with-real-value/?_php=true&_type=blogs&_r=0

〔47〕*See* Nathaniel Popper, *Move Over, Bitcoin. Ether Is the Digital Currency of theMoment*, N.Y. TIMES DEALBOOK (June 19, 2017), https://www.nytimes.com/2017/06/19/business/dealbook/ethereum-bitcoin-digital-currency.html.

型的两个例子就是超级账本(Hyperledger)[由 Linux 基金会(LinuxFoundation)赞助的开源式项目][48]和 R3 金融服务联盟(R3 financialservicesconsortium)。[49]

各平台采用的技术方法大同小异。为对不同因素(例如,性能、去中心化、合规性、匿名化、安全性以及功能性)进行优化,各平台在设计上有所取舍。未来,或许只会存在一条主要的区块链,或多个主要平台和成千上万的小平台。就代币市值而言,比特币仍是最大的平台,但其支配地位似乎岌岌可危。未来二十年,比特币可能价值千金,也可能一文不值。但随着市场发展,比特币代表的区块链结构也日趋完善。此类系统均包含以下三个主要特征:分布式分类账、共识和智能合约。

1.分类账

分类账指账目记录。最为人熟知的就是使用复式记账法(会计的基础)的分类账。然而,分类账的用途并不仅限于记录公司资产负债表中的借贷情况。[50]房地产市场离不开土地所有权登记,民主要求分类账计算投票,著作权利用公共和私人记录来追踪权利登记和转让。现代公司不仅利用分类账处理其财务,还以此调节内部代理人与外部合作伙伴的关系,以及供应链、后勤部门和面向客户活动的关系。马克斯·韦伯和维尔纳·桑巴特等社会学家指出,复式记账法是现代资本主义的基础。[51]

区块链是一种分布式分类账。[52]任何该网络的参与者均可保留分类账的副本,关键是所有副本的内容完全相同。风险投资者阿尔伯特·温格(Albert Wenger)提出,区块链在逻辑上是中心化的(因为只有一份分类账),但在组织结构上却是去中心化的(多个实体均保有该分类账的副本)。[53]区块链系统的各节点为保持同步,彼此相互联系。由于并无规范的原本作为参照,保持同步(也称共识)才是难点所在。

中心化分类账本身也有弱点。一方面,若由单一节点保存主分类账,则这一节点就是整个系统的唯一故障点,任何其他节点的使用者都无法确认所见信息的准确性。另一方面,若各组织分别保存自己的分类账(和大多数公司的财务记录一样),则每笔交易至少会被单独记录两次。举例而言,公司向供应商付款或银行为其他银行客户兑换支票时,双方均需通过对账程序同步其分类账。这会加大交易的复杂性,引发交易延迟或错误。区块链问世之前,这些问题被认为是难以避免的。[54]

[48]*See* Todd Benzies, *Tech and Banking Giants Ditch Bitcoin for Their Own Blockchain*, WIRED. COM (Dec. 17, 2015), https://www.hyperledger.org/news/2015/12/17/wired-tech-and-banking-giants-ditch-bitcoin-for-their-own-blockchain.

[49]*See* Paul Vigna, *Blockchain Firm R3 CEV Raises $107 Million*, WALL ST. JOURNAL (May 23, 2017, 6:37pm ET), https://www.wsj.com/articles/blockchain-firm-r3-raises-107-million-1495548641.

[50]*See* Dominic Frisby, *In Proof We Trust*, AEON (Apr. 21, 2016),https://aeon.co/essays/how-blockchain-will-revolutionise-far-more-than-money.

[51]*See* MAX WEBER, GENERAL ECONOMIC HISTORY 276 (Trans. Frank H Knight, 1927)("现代资本主义存在的最普遍的前提就是合理的资本核算……"); WERNER SOMBART, DER MODERNE KAPITALISMUS 23 (1916)("资本主义和复式记账绝对不能分割;它们两者是形式与内容的关系"). *See* also Quinn DuPont and Bill Maurer, *Ledgers and Law in the Blockchain*, KING'S R EVIEW (June 23, 2016), http://kingsreview.co.uk/magazine/blog/2015/06/23/ledgers-and-law-in-the-blockchain/(详细说明了分类账的重要性以及对区块链的影响).再向前追溯,许多现存最早的美索不达米亚楔形文字的古代书面文件都是商业交易的分类账。*See* HANS J. NISSEN, PETER DAMEROW, AND ROBERT K. ENGLUND, ARCHAIC BOOKKEEPING: EARLY WRITING AND TECHNIQUES OF ECONOMIC ADMINISTRATION IN THE ANCIENT NEAR EAST (Univ. of Chicago Press 1993).

[52]*See* UK Government Chief Science Advisor, supra note 37; PAUL VIGNA & MICHAEL J. CASEY, THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER 124 (2015). 并非所有分布式分类账都是区块链的结构。例如,受监管银行之间的金融协议使用的 Corda 系统使用的就是一种不同的数据结构。*See* Richard Gendal Brown, Introducing R3 Corda (TM): *A Distributed Ledger Designed for Financial Services*, Richard Gendal Brown blog (April 5, 2016), https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/. 但区块链是最常用的结构,尤其是对于公共(无需许可)系统而言,因此这里使用"区块链"这个术语。

[53]Albert Wenger, Bitcoin: *Clarifying the Foundational Innovation of the Blockchain*, Continuations (Dec. 15, 2014), http://continuations.com/post/105272022635/bitcoin-clarifying-the foundational-innovation-of.

[54]对分布式数据库系统进行广泛研究和大量部署已持续多年。但是,这些系统通常假设所有节点将由单个公司控制。它们担心节点出现故障引发危险,而区块链系统可以防止不可靠节点攻击系统。*See* Rajesh Nair, *Why Aren't Distributed Systems Engineers Working on Blockchain Technology?*, PAXOS ENGINEERING BLOG (Aug. 1, 2017), https://eng.paxos.com/why-arent-distributed-systems-engineers-working-on-blockchain-technology.

2.共识

比特币的核心是一系列软件协议，通常被称为中本聪共识。[55]共识指网络参与者确信其分类账准确一致。[56]若无强力手段保障共识，比特币参与者就能重复使用比特币（即重复消费问题），或谎称其拥有更多代币。大多数数字化系统共识的达成方法都有一个通病，即很容易产生大量虚假网络节点，也就是所谓的“女巫攻击”（Sybilattack）。[57]即使大部分的实际用户都是诚信的，攻击者仍可伪造足够的节点控制网络，并在系统执行错误的共识。这就是密码学领域著名的“拜占庭将军问题”（Byzantine Generals Problem）。[58]

中本聪巧妙地将密码[59]技术与博弈论[60]观点相结合，对这一问题作出解答。首先，所有比特币交易的签署均应经过加密处理。只有相关私钥（由字母和数字组成的秘密字符串）的持有人才能发送相关信息，这一点在数学上是可行的。其次，比特币和其他共识系统以信任网络取代了信任个体。行为主体（在比特币系统中被称为矿工）负责查验交易。[61]任何人都可以成为矿工。即使其中有些人并不可信，但只要大部分人是诚信的，系统便可正常运转。[62]在中本聪看来，矿工竞相验证大块的比特币交易，也就是区块。[63]每一区块的赢家会得到奖励。

对这一系统，“女巫攻击”是主要问题。若不守信行为难度低回报高，有人变节是必然的。为解决这一问题，比特币领域的第二项加密技术——工作量证明——应运而生。[64]工作量证明大大提高获得交易验证权的难度。比特币系统要求矿工解决涉及单向函数的密码问题（也称哈希）。[65]解决上述

〔55〕*See* Joseph Bonneau et al, *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, in Proceedings of the 36 th IEEE Symposium on Security and Privacy, http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf, at 3; Nick Szabo, The Dawn of Trustworthy Computing, UNENUMERATED （Dec. 11, 2014）,http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html.

〔56〕关于共识的重要性的具体讨论，*see* Casey Kuhlman, *What Are Ecosystem Applications*, ERIS INDUSTRIES BLOG（June 5, 2016）,https://db.erisindustries.com/eris/2016/06/05/ecosystem-applications/ （“区块链技术所解决的问题既不是电子 P2P 现金，也不是结算延迟，而是入站事件的归因和排序……”）。

〔57〕*See* John R. Douceur, The Sybil Attack, IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems 251（2002）, http://nakamotoinstitute.org/static/docs/the-sybil-attack.pdf.

〔58〕*See* Leslie Lamport, Robert Shostak & Marshall Pesce, *The Byzantine Generals Problem*, 4.3 ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS 382（1982）.这个名词是指在一个假想的场景中，一群来自拜占庭帝国的将军包围了一座城市，但他们彼此之间不能有效地协调行动。

〔59〕密码学是数学技术在通信安全保障方面的一种运用。加密是密码学的一部分，用以确保信息仅在使用密钥时方可读取。比特币的核心协议实际上并没有加密。交易处于公开但安全的状态。

〔60〕在同一时间内，其他人也提出了相似的方法，但没有一种方法能以强有力的手段达成共识。例如，密码学家 Nick Szabo 提出了一个名叫 BitGold 的系统。Nick Szabo, *Liar-Resistant Government*, U NENUMERATED （May 7, 2009）, http://unenumerated.blogspot.com/2009/05/liar-resistant-government.html.

〔61〕这种方法类似于以美国为代表的国家所采用的共和制政府形式。国家权力分散给公众，通过投票行使，而非交由国王独享。为了避免党派之争和暴民统治，选民通过选举自己的代表来间接行使权力。*See* Hyperledger Architecture, Volume 1, at 4（2017）, https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper 1 Consensus.pdf.

〔62〕安全研究人员已经确定，不诚信矿工必须控制大约三分之一的网络计算能力才能成功攻击系统。即便三分之一不是多数，但这已意味着非常重大且昂贵的投入。

〔63〕Bitcoin: *The Magic of Mining, ECONOMIST*, Jan. 10, 2015, at 58,http://www.economist.com/node/2163812; ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES（2014）. See also Kevin Werbach, Bitcoin is Gamification, MEDIUM,（Aug. 5, 2014）, https://medium.com/@kwerb/bitcoin-is-gamification-e85c6a6eea22（解释动机系统对比特币的重要性）.

〔64〕*See* Narayanan et al, supra note 37, at 266. 并不是每个区块链都像比特币一样使用工作量证明技术。例如，以太坊（Ethereum）使用一种改进的算法，这样一来，矿工便不能从使用一种称为 ASIC 的定制芯片中获益。其他分布式分类账平台，如 Ripple 和 Tendermint，也根本没有使用工作量证明技术，而是用一种替代机制来达到同样的目的。*See* Bonneau et al, *supra note55*.但这些共识协议是否和比特币使用的工作量证明技术一样有效还有待观察。See id.

〔65〕一个哈希函数需要一些输入字符串（例如一个文件）然后将其转换为具有一定长度的输出字符串——哈希值。虽然在理论上可能会出现多个输入字符串可以映射到相同的哈希值上，但是密码哈希值空间足够大，以致出现这种“碰撞”的可能性是极小的。计算任何一个文件的哈希函数是非常容易的。一个输入字符串每次都会产生相同的输出字符串。但是现在还没有一个已知的方法能够将哈希值还原为原始数据，除非反复尝试。*See* Narayanan et al, *supra note37*, at 23-24.矿工必须尝试十分大量的哈希值才能找到产生特定输出结果的字符串。*See id*. at 61-68.

问题需要巨大的且不断增长的计算能力,这一硬件要求令"女巫攻击"难如登天。[66]欺骗系统的代价远超其收益。其他共识系统包括权益证明(该系统中,若验证人试图欺骗系统,就可能失去所有代币)和不要求"风险共担"的投票和彩票算法,例如瑞波共识协议(Ripple Consensus Protocol)。[67]

通过在区块中聚集交易,共识对单笔个人交易以及分类账整体的完整性予以确认。[68]工作量证明系统会进行动态调整,每十分钟生成一次区块哈希难题的有效答案。[69]经验证的每一区块均以上一区块的哈希为密码签名,以此组成一条稳定的连续区块链。最长的链代表该系统的共识状态。[70]攻击者只有掌握整个网络绝大部分的计算能力才能建立起"欺骗性区块",并以之"分叉"最长链(也称51%攻击)。[71]因此,区块的位置越靠前,"分叉"难度就越大。

公共区块链(例如比特币区块链)会记录网络上所有交易,且对全体参与者公开透明。[72]不仅比特币区块链的内容向所有人公开,相关的软件也为开源式的,可免费获取。[73]比特币还具有抗审查性和防篡改性。不存在任何政府可以操纵或拦截的中央控制点或网络。一旦一笔交易被记录下来,该记录就是不变的,这一特性也被称为恒定性。用户甲可向用户乙赠送比特币,用户乙也能够返还全部或部分,但用户甲、矿工或任何其他人都不能撤销最初的赠币行为。[74]

这些特点彰显的开放性和去中心化与早期网络(而非如今管控较严的网络环境)类似。[75]似乎能够实现某些互联网先锋对劳伦斯·莱西格所说的不可监管技术领域的梦想。[76]

中本聪共识的最后关键部分就是博弈论或心理学观点:验证区块吃力不讨好,矿工何苦为之?毫不夸张地说,工作量证明代价极高:需要特定的计算硬件和大量的电力供给。仅仅是为他人谋利不足以令矿工变节。中本聪的处理方式非常巧妙。成功验证区块的矿工能够获得可观的奖励,即比特币。许多问题因此迎刃而解,包括货币如何在没有中央银行的情况下进入货币供应的问题。由于新的比特币只能通过奖励机制产生,生成率必定会逐渐下降。[77]因此,矿工验证区块虽然是出于个人利益,但同时也造福整个社群。

因此,比特币既是系统的输出,也是其输入。其既是支持数字货币的信任基础架构,也是支持信

〔66〕随着互联网计算能力的提升,其难度级别还会自动调整。今天的比特币网络比500台当今最强大的超级计算机加起来还要强大。*See* Laura Shin, *Bitcoin Production Will Drop By Half In July, How Will That Affect The Price?*, FORBES (May 24, 2016, 7:30am), http://www.forbes.com/sites/laurashin/2016/05/24/bitcoin-production-will-drop-by-half-in-july-how-will-that-affect-the-price/#46f73a5499e1. 其所需要的计算能力如此之大,人们开始担忧为了支持和冷却数据中心所需要的电力带来的环境影响。*See* Tapscott & Tapscott, *supra note*37, at 259–63.

〔67〕*See* Hyperledger Architecture, *supra note* 61.

〔68〕*See* Narayanan et al, *supra note* 37, at 88–90.

〔69〕*See id*. at 65.

〔70〕*See id*. at 59. 更确切地说,是最长的工作量证明链。

〔71〕一些研究表明,具备三分之一采矿能力的攻击者能够破坏网络。但是,这仍然是一个很高的门槛。

〔72〕在区块链中,用户的身份是通过电子签名得到确认的,因此交易双方在真实世界中的身份也许无法确定。对于那些希望进一步匿名的人来说,可以通过分散交易来掩盖大额交易。

〔73〕Alec Liu, *Who's Building Bitcoin? An Inside Look at Bitcoin's Open Source Development*, M OTHERBOARD (May 7, 2013, 12:20pm EST), http://motherboard.vice.com/blog/whos-building-bitcoin-an-inside-look-at-bitcoins-open-source-development.

〔74〕比特币系统使用被称为"未使用交易输出"(UTXO)的机制来记录交易,而非记录资产持有量。这使得即使大多数矿工改变他们的比特币软件来放松对特定区块的验证,也难以使账户余额恢复到之前的状态。其他一些加密货币平台更容易"硬分叉",以便恢复之前的交易,因为它们在账户而不是UTXO上操作。以太坊(Ethereum)社区在2016年7月就是这样做的,旨在解决从名为The DAO的众筹平台窃取货币的问题。*See* infra text at notes 126–132. 但这种做法是有争议的,因为它们使公共区块链的审查抵制和不变性受到了质疑。

〔75〕*See* Andreessen, *supra note* 37; Morgen E. Peck, *The Future of the Web Looks a Lot Like Bitcoin*, IEEE S PECTRUM (July 1, 2015), http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin.

〔76〕Lawrence Lessig, Deja Vú All Over Again: Thinking Through Law & Code, Again, VIMEO, https://vimeo.com/148665401.

〔77〕因此,类似于在现实世界中挖掘先前的资源。最终区块奖励将降至零。此时,流通中的比特币数量将固定为2100万。中本聪(Nakamoto)预计,随着比特币系统应用的风靡,寻求验证者向矿工自愿支付的交易费用将逐渐取代奖励。但这仍有待观察。

任基础架构的数字货币。

3.智能合约

分布式分类账是主动而非被动的。换言之,分布式分类账不只记录传递给其的信息。作为共识系统的一部分,其必须确保记录的交易已经完成,与共识相匹配。〔78〕就比特币而言,这意味着系统会自动执行财务汇款。〔79〕用户不能发起赠发比特币的交易,然后又反悔;汇款对账和达成的同步也是交易程序的一部分。这一机制被称为智能合约。〔80〕权利和义务规定以及契约协议的执行都在该平台有所体现。

智能合约这一概念早于比特币产生,是专属于区块链的概念。〔81〕但在中本聪发布论文之前,这两个概念风马牛不相及。比特币利用智能合约来进行交易,智能合约则利用比特币的分布式分类账来运作自治权。从技术角度看来,智能合约本质上是自治软件媒介。〔82〕有了智能合约,分布式分类账能够实现分布式计算机的功能。同样的共识算法(这一算法下,各节点均可获得分类账的相同副本)使得智能合约以恒等顺序进行恒等计算。比特币以智能合约为运行基础,为保证安全性,严格限制智能合约的基本资金能力。

现今最著名的智能合约平台就是 2015 年推出的以太坊。〔83〕以太坊提供一种图灵完备的编程语言,理论上来讲,在普通电脑上运行的任何应用均可在以太坊共识网络的分布式电脑上运行。〔84〕正如网络和各种基础设施工具(例如应用服务器)是谷歌、亚马逊和易趣的基础,开发者可在以太坊平台编写新的应用程序。以太坊的加密货币以太币是继比特币之后最具价值的加密货币。〔85〕

一般的智能合约平台是去中心化应用(也称 DApps)的基础。〔86〕就区块链的财务用途而言,许多去中心化应用都模拟了现有的中心化应用。星际文件系统(IPFS)和 Storj 提供了与 Dropbox 和苹果的 iCloud 类似的去中心化云存储服务;〔87〕Decent 提供类似于博客和音乐发行服务的去中心化内容发布

〔78〕比特币实际上使用脚本语言进行交易,这意味着每次转账实际上是在区块链上运行软件代码。*See* Narayanan et al, *supra note* 37, at 79–889(描述比特币脚本语言和一些不仅仅进行基本现金转移的应用程序).

〔79〕确切地说,区块链记录了创造或破坏比特币的挑战和反应,而不是传输这些离散的代币。*See* Narayanan et al, *supra note* 37, at 75–76.

〔80〕*See* Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 2 FIRST MONDAY (1997), http://ojphi.org/ojs/index.php/fm/article/view/548; TIM SWANSON, GREATC HAIN OF NUMBERS: AGUIDE TO SMART CONTRACTS, SMART PROPERTY AND TRUSTLESS ASSET MANAGEMENT 67 (2014); Nick Szabo, *The Idea of Smart Contracts* (1997), http://szabo.best.vwh.net/smart_contracts_idea.html; Wright and De Filippi, *supra note* 23, at 24–26; Werbach & Cornell, supra note 25; Raskin, supra note 25.

〔81〕*See* Szabo, *supra note* 80.

〔82〕*See* Vitalik Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, GITHUB, https://github.com/ethereum/wiki/wiki/White-Paper.

〔83〕*See id.*; Popper, *supra note* 47; D.J. Pangburn, *The Humans Who Dream of Companies That Won't Need Us*, FA COMPANY (June 19, 2015), http://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-need- them; Jim Epstein, *Here Comes Ethereum, an Information Technology Dreamed Up By a Wunderkind 19-Year-Old That Could One Day Transform Law, Finance, and Civil Society*, REASON.COM (Mar. 19, 2015), http://reason.com/blog/2015/03/19/here-comes-ethereum-an- information-techn; Tina Amirtha, *Meet Ether, the Bitcoin-Like Cryptocurrency That could Power the Internet of Things*, FAST COMPANY (May 21, 2015), http://www.fastcompany.com/3046385/meet-ether-the-bitcoin-like-cryptocurrency-that-could- power-the-internet-of-things.

〔84〕分布式共识的开销意味着此类应用程序的运行速度可能远远低于单台计算机或 Amazon Web Services 等云计算平台上的运行速度。

〔85〕Nathaniel Popper, *Ethereum, a Virtual Currency, Enables Transactions That Rival Bitcoin's*, N.Y. TIMES DEALBOOK (Mar. 27, 2016), http://www.nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enables- transactions-that-rival-bitcoins.html?_r=1.

〔86〕截至 2016 年 7 月,一个站点列出了处于各个发展阶段的 500 多个分散式应用项目。STATE OF THE DAPPS, http://dapps.ethercasts.com/.

〔87〕*Storj, the New Decentralized Cloud Storage Platform Goes Live*, NEWSBTC (Apr. 10, 2016, 4:30pm), http://www.newsbtc.com/2016/04/10/storj-new-decentralized-cloud-storage- platform-goes-live/; Ian Allison, How IPFS is Reimagining the Internet, Newsweek (Oct 21, 2016, 12:08pm), http://www.newsweek.com/how-ipfs-reimagining-internet-512566.

服务;[88]Commuterz 则与优步和来福车相同,支持去中心化的共享出行服务;[89]OpenBazzar 则与易趣类似,同样是去中心化的电子商务市场,但其以比特币为交易货币。[90]

其他 DApps 则更具新颖性。例如,高盛集团指出,区块链对发展分布式电力市场大有裨益。[91]使用者可以将屋顶太阳能电池生成的剩余电力转卖给当地的电力公司。由于个人客户和电力公司的潜在交易数量巨大,管理开销自然不菲,因而如今对此类交易的限制比较严格。[92]分布式分类账能够在没有中央系统开支的情况下,追踪上述交易。高盛集团预测,这会带来每年 25 到 70 亿美元的市场机遇。[93]

DAO 是最具潜力的去中心化应用。[94]在 DAO 中,对股权、债务和公司治理标准的公司安排会被编码为一系列智能合约。[95]投资者可以加密货币的形式进行注资,而分布式应用将会对工资、股息和代理投票等事项的支付进行处理。"DAO"这一曾遭毁灭性攻击的众筹系统被定义为区块链概念的初体验。[96]

(二)适用的理由

若分布式分类账不能解决实际问题,则其仅对译码者或哲学家有意义。区块链的适用一定程度上受到意识形态领域规避国家控制观点的驱动。然而,当下大多数对区块链展开研究调查的创业者、大公司、主要的金融机构和政府都追求实际利益。区块链的两个主要价值主张分别为:避免依赖中央行为主体和在相互猜忌的个体中建立普遍诚信。

1.避免与中央机关的矛盾

2016 年,阿根廷布宜诺斯艾利斯当局禁止信用卡公司处理优步(网约车公司)的交易,因该公司违反了地方法规。发行比特币借记卡的 Xapo 能够规避上述禁令,[97]因其并不要求从本地连接传统支付平台。优步可以无视禁令,继续营业。

至于以这种方式规避监管恰当与否,仁者见仁,智者见智。但至少在某些情况下,不依赖中央行为主体的确难能可贵。这也是拉美国家积极采用比特币作为支付手段的原因。[98]经历过恶性通货膨

〔88〕http://decent.ch/.

〔89〕http://commuterz.io.

〔90〕*See* Andy Greenberg, The Fed-Proof Online Market OpenBazaar is Going Anonymous, Wired.com (March 6, 2016, 7:00am), https://www.wired.com/2017/03/fed-proof-online- market-openbazaar-going-anonymous/.
See Schneider et al, *supra* note 15, at 4.

〔91〕*See* Schneider et al, *supra* note 15, at 4.

〔92〕纽约布鲁克林正在进行此类试验计划。*See* Aviva Rutkin, *Blockchain-Based Microgrid Gives Power to Consumers in New Nork*, NEW SCIENTIST (March 9, 2016), https://www.newscientist.com/article/2079845-blockchain-based-microgrid-gives- power-to-consumers-in-new-york/.

〔93〕*See* Schneider et al, *supra* note 15.

〔94〕*See* Vitalik Buterin, *Bootstrapping A Decentralized Autonomous Corporation: Part I*, BITCOIN MAG. (Sept. 19, 2013), https://bitcoinmagazine.com/7050/bootstrapping-a- decentralized-autonomous-corporation-part-i/; MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY (2015; Wright and De Filippi, *supra* note 23, at 17, 31-32.

〔95〕这些虚拟公司的法律地位以及他们的投资者、开发商和受益人的地位是一个悬而未决的问题。*See* Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 Nw. U. L. Rev. 1483 (2014); Tanaya Macheel,DAO 可能是开创性的,但它是否合法? AM. BANKER (May 19, 2016)http://www.americanbanker.com/news/bank-technology/the-dao-might-be- groundbreaking-but-is-it-legal-1081084-1.html; Peter Van Valkenburgh,DAO:*the Internet is Weird Again, and These are the Regulatory Issues*, COINCENTER (June 2, 2016), https://coincenter.org/entry/daos-the-internet-is-weird-again-and-these-are-the-regulatory- issues.

〔96〕*See* supra note 24-30 and accompanying text.

〔97〕*See* Jamie Redman, *Uber Thriving in Argentina Once Again Thanks to Bitcoin*, BITCOIN.COM NEWS (July 9, 2016), https://news.bitcoin.com/uber-thriving-argentina-bitcoin/; Joel Valenzuela, *Uber Switches to Bitcoin in Argentina After Govt Blocks Uber Credit Cards*, COINTELEGRAPH (July 6, 2016, 11:40am), http://cointelegraph.com/news/uber-switches-to- bitcoin-in-argentina-after-govt-blocks-uber-credit-cards.

〔98〕*See* Sonny Singh and Alberto Vega, *Why Latin American Economies are Turning to Bitcoin*, TECHCRUNCH (March 16, 2016), https://techcrunch.com/2016/03/16/why-latin- american-economies-are-turning-to-bitcoin/.

胀和货币贬值，民众对政府和金融制度的信心大打折扣。通常认为，比特币能够不受政治变迁和国际贷款机构需求的影响，因此其似乎是更加保险的选择。比特币的价值主张之一就是成为一种优于黄金的剩余价值储存手段，当下黄金的资产类别已达 7 万亿美元。〔99〕

当中央个体行为主体参与其中时，适用同样的机制。信任会带来风险。信任一个不可信的人往往是十分危险的。伯纳德·麦道夫（Bernie Madoff）认为，庞氏骗局的投资者就是因为信任错的投资经理才倾家荡产。〔100〕法律、法规和保险都是限制此类风险的机制。至少在美国，麦道夫的情况是例外，而不是规则。然而，对于受放高利贷者、发薪日贷款机构或敲诈勒索销赃人辖制的人而言，区块链提供了其更好的选择。

即使被信任的权威机构具有一定可信度，其仍是会受到攻击的单一故障点。例如，加密证书仅对用户连接网站的正确性加以验证，并不干涉其他事项，以此确保访问网址的安全性。前述证书由中央证书授权机构签发。2011 年，DigiNotar，一家荷兰证书授权机构，受到黑客攻击。〔101〕黑客伪造了多个虚假证书，拦截并重新定向谷歌 Gmail 服务及其使用者之间的流量。虽然谷歌和网络浏览器供应商迅速行动，作废虚假证书，将损失限制在可控范围内，但这一事件反映出中心化系统的风险。〔102〕域名币、以太网名称服务和 Blockstack 之类的项目旨在创建访问线上资源的安全结构，规避上述问题。〔103〕

此外，所有中介都收取费用。当中介机构为私营公司的，希望从其创造的价值中获得收益。谷歌向其用户推送广告以及精准定位投放广告，以此向广告商收取费用。如今的广告年收益已达数百亿美元，是典型的直接中介费用。若搜索引擎广告市场可以脱离谷歌而存在，则无需支付上述费用。随着中介机构数量成倍增长，费用也相应增长。举例而言，搜索引擎优化公司就是依附于谷歌而存在的中介机构。这些公司为其所提供的服务收费，而谷歌则需要耗费大量的资源来避免过度依赖搜索结果。

为服务自身利益，中介机构不断改造市场。若无利益，他们就会限制行为或停止创新。2017 年，欧盟以操纵线上购物搜索结果帮助附属公司谋利为由，对谷歌处以 27 亿美元的罚款。〔104〕就本质而言，成为某一社群的信任核心势必会形成垄断势力。例如，许多网站使用脸书的“社群登录”服务来核验其用户的认证信息。由于脸书是在线社群互动的可信中介，由其运作身份管理程序必定会事半功倍。但社群登录也确立了脸书的控制权。〔105〕令脸书可以获得超出其平台范围的数据并设置竞争障碍。和脸书一样长期占据中心地位的公司和所有垄断机构一样，都试图抬高价格，延缓创新。此种垄断机构往往从其创收中牟利。然而，该网络中的其他人则需要缴纳税赋，且有时是重税。

2.普遍诚信

区块链在速度和效率方面潜力巨大。初看上去，这种说法略显奇怪。比特币每十分钟验证一个区块，每秒钟交易数量的理论上限为 7 笔。这一数值非常不起眼：Visa 信用卡网络每秒交易数量达到

〔99〕*See* Nathan Lewis, *Gold Or Bitcoin? Gold And Bitcoin*, FORBES (June 30, 2017, 11:59am), https://www.forbes.com/sites/nathanlewis/2017/06/30/gold-or-bitcoin-gold-and- bitcoin/#3a6f0fe33e4b.

〔100〕麦道夫的一部重要传记的副标题是“Bernie Madoff and the Death of Trust.” DIANA B. HENRIQUES, THE WIZARD OF LIES (2011)。

〔101〕*See* Kim Zetter, *Diginotar Files for Bankruptcy in Wake of Devastating Hack*, WIRED.COM (Sept. 20, 2011, 3:05pm), https://www.wired.com/2011/09/diginotar-bankruptcy/.

〔102〕*See* Josephine Wolf, *How a 2011 Hack You've Never Heard of Changed the Internet's Infrastructure*, SLATE FUTURE TENSE (Dec.21,2016, 11:00am), http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of_digin otar_changed_the_internet_s_infrastructure.html.

〔103〕*See* Michael del Castillo, *Blockstack Releases Blockchain-Powered, Tokenized Internet Browser*, COINDESK (May 23, 2017, 13:52 UTC), https://www.coindesk.com/blockstack- blockchain-decentralized-browser/.

〔104〕*See* Mark Scott, *Google Fined Record $2.7 Billion in E.U. Antitrust Ruling*, N.Y. TIMES, June 27, 2017, https://www.nytimes.com/2017/06/27/technology/eu-google-fine.html.

〔105〕*See* generally Julie Cohen, *Law for the Platform Economy*, UC DAVIS L. REV. (forthcoming 2017)（讨论数字平台如何利用互联网环境来聚合权力）.

10000 笔。〔106〕同步分布式分类账的开销十分巨大,依照译码者尼克·萨博的估计,区块链同步程序的运行速度比一般电脑慢 10000 倍。〔107〕

但无需信任与自身有联系的特定行为主体具有一项潜在优势。信任是不可传递的。甲信任自己的银行,但这并不意味着他需要信任乙的银行。若甲要兑换乙的支票,则双方的银行需要建立各自的信任关系。随着成千上万的金融机构在世界各地处理数十亿美元的交易,这种成对结构很快举步维艰。更准确地说,这种结构效率低下且交易成本较高。很多时候,对于受信任行为主体而言,交易费用其实是进一步价值提取机会。因此为汇款和信用卡提供商带来巨大收益。〔108〕对多个相关受信任方之间的交易进行核验是一项极其复杂的任务,进一步延长核验程序。举例而言,股票交易通常在交易达成之后 3 日内进行结算(被称为 T+3 标准)。〔109〕而被占用的资金原本可以被更有效地利用。

事实上,这一模式和区块链模式均创制了去中心化分类账。传统制度中,各个节点独立负责保存其分类账,并与虚拟共识保持一致,且仅有直接合作伙伴可见。在区块链中,每增加一个区块,都会对整个系统的交易进行核对。该区块能够有效并行数个序列程序。记录单笔交易会耗费很长时间,但系统状态的全球更新反而非常迅速。由于上述记录和更新是通过同一个同步程序而非大量独立交易展开的,因此成本大大降低。〔110〕据高盛集团预测,在证券交易的结算和核对费用方面,区块链每年能够节省 110—120 亿美元。〔111〕

比特币和其他区块链系统的确面临巨大的挑战。比特币开发社区就相关机制展开争论,例如要不要扩大各个区块的规模来提升系统表现。〔112〕相比之下,现行的金融制度经长期优化,能够稳定开展大规模交易。有人预测,区块链很快就能横扫银行系统,这种说法显然言过其实。然而,提升对账的速度和效率是各大金融机构积极探索许可区块链的主要原因之一。

最后,构建分布式分类账的方法很多。〔113〕在公共区块链中,例如比特币和以太坊,任何人均可运行一个挖掘节点,并保存共享分类账的副本。由于无法查验网络参与者的完整性,详细的协议(例如中本聪共识)和所有交易信息的高开销分布就十分必要。许可分类账可以消除这些限制,更有效地运作,但代价是重新引入中央控制的要素。〔114〕使用情况不同,解决方法自然不同。

2009 年比特币问世,开启分布式分类账的时代,但仍处于初级阶段。2017 年 3 月,以太坊核心开发者弗拉德·赞菲尔发布一条推文:“以太坊并不安全,且不具扩展性。其只是不成熟的实验性科技。如非必要,切勿在其上运行关键任务应用!”此言一出,举座皆惊。〔115〕但其所言非虚,且不仅仅针对以

〔106〕*See* Timothy B. Lee, *Bitcoin Needs to Scale by a Factor of 1000 to Compete with Visa. Here's How to Do it*, WASH. POST THE SWITCH BLOG (Nov. 12, 2013),https://www.washingtonpost.com/news/the-switch/wp/2013/11/12/bitcoin-needs-to-scale-by-a-factor-of-1000-to-compete-with-visa-heres-how-to-do-it/.新技术可能会大大提高比特币交易网络的速度。*See* Romain Dillet, *Blockchain Open Sources Thunder Network, Paving the Way for Instant Bitcoin Transactions*, TECHCRUNCH (May 16, 2016), https://techcrunch.com/2016/05/16/blockchain-open-sources-thunder- network-paving-the-way-for-instant-bitcoin-transactions/.

〔107〕*See* Nick Szabo, *The Dawn of Trustworthy Computing*, UNENUMERATED (Dec. 11, 2014), http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html.

〔108〕全球的汇款市场一年产生 380 亿美元的费用。*See* Tapscott & Tapscott, *supra* note 37, at 183.

〔109〕*See* John McCrank, *Settlement Time for U.S. Trades Closer to Being Shortened*, REUTERS (Apr. 23, 2014, 9:03am EDT), http://www.reuters.com/article/us-markets-clearing- dtcc-idUSBREA3M10920140423.

〔110〕*See* Building the Trust Engine, *supra* note 37, at 9, 18.

〔111〕*See* Schneider et al, *supra* note 15, at 5.

〔112〕*See* Narayanan et al, *supra* note 37, at 98.

〔113〕关于公共和权限分类帐之间的差异的讨论,*see* Swanson, *supra* note 80。

〔114〕*See* Richard Gendal Brown, *Towards Deeper Collaboration in Distributed Ledgers: Thoughts on Digital Asset's Global Synchronisation Log*, THOUGHTS ON THE FUTURE OF FINANCE (Jan. 24, 2017), https://gendal.me/2017/01/24/towards-deeper-collaboration-in- distributed-ledgers-thoughts-on-digital-assets-global-synchronisation-log/.

〔115〕Zamfir 第二天即在一篇更长的文章里对此作出解释。*See* Vlad Zamfir, *About My Tweet from Yesterday..*, MEDIUM (March 5, 2017), https://medium.com/@Vlad_Zamfir/about-my-tweet-from-yesterday-dcc61915b572.

太坊。无数正在展开的合理措施、经典的使用案例、主要企业的支持和各方注入的资金都证明，区块链并非昙花一现。尽管区块链的发展趋势尚不明确，其潜在利益仍不可限量，但同时也伴随严重风险和公共政策挑战。

三、分类账与法律

分布式分类账令用户可以放心存储和交换贵重资产，但这与信任特定个体或机构不可混为一谈。〔116〕若区块链完全改变传统的信任模式，以信任软件代码和密码取代信任人、公司和政府，只会适得其反，引发不信任。这种不协调会造成严重后果。当中本聪的精妙数学构思遭遇混乱无序的实际实施，似乎就跌落神坛，不再完美。若区块链被定位成唯一的执行担保手段，其局限性必定会引发问题。幸好有一种机制可以与区块链技术信任机制结构相互配合，这种机制就是法律。

（一）可能出现的问题

自诞生以来，比特币共识分类账从未被成功攻破。富有经验的攻击者几经尝试，均以失败告终。比特币实际上就是钱，分类账就如同一个银行金库。2017 年中期，其储存金额超过 500 亿美元。保证这笔财富安全无虞是区块链技术有效运行的最好证明。然而，尽管比特币和其他主要区块链系统能有效规避重大安全故障，但加密货币的安全并非绝对。随着环境的变化，这种安全能否延续尚未可知。2015 年，一些主要的研究者指出："我们对比特币的理解还不够深入，不足以对比特币能否继续良性运转下定论。"〔117〕

把区块链网络看作一系列同心圆。中心位置是分类账，以稳健的去中心化共识保证其安全性。第二个同心圆是智能合约，是引导该网络交易的软件代码。第三个同心圆是交易所和钱包服务之类的边缘服务供应商，是加密货币和现实世界之间的桥梁。最外围是去中心化应用和其他应用直接向用户销售的代币。每层都各有其弱点。

1.信任分类账

区块链系统并非无懈可击。区块链系统以现代密码技术为基础。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。〔118〕然而，若此类弱点继续存在，势必会影响同样以密码学为基础的线上交易系统。此外，区块链已经吸引多名世界顶级的密码学家，他们正积极探索解决上述问题的方法。另一隐患就是密码技术的实施不完善，例如密码利用随机数生成器生成数字，但其生成数字的方式并不是随机的。区块链技术和其他以计算机代码为基础的系统一样，都不完美。经证实，开源式比特币代码存在重大缺陷，尽管这些缺陷在出现持久损害之前就被解决了。

挖矿或工作量证明程序存在更严重的漏洞。中本聪对"拜占庭将军"问题提出了有力的解决方案，但仍无法解决 51%攻击的问题。〔119〕若某人能够控制网络内超过一半的挖矿能力，就能随意选择验证任一区块，即使存在重复消费的行为。聚集起如此巨大的处理能力并非易事，这也是比特币系统

〔116〕协议并不一定意味着信任。对博弈论的一种认识是，即使是非交流方也可以通过独立选择最可能或最熟悉的选项来达成共识。*See* THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT （1960）. 智能合约和以太坊的创造者都参考了这些 Schelling Points。*See Szabo, supra* note 80; Vitalik Buterin, *SchellingCoin: A Minimal-Trust Universal Data Feed*, ETHEREUM BLOG（March 28, 2014）, https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/.

〔117〕*See* Bonneau et al, *supra* note 55, at 1.

〔118〕*See First Quantum-Secured Blockchain Technology Tested in Moscow*, MIT TECH. REV., June 6, 2017, https://www.technologyreview.com/s/608041/first-quantum-secured- blockchain-technology-tested-in-moscow/。

〔119〕虽然 51%的攻击是最被广泛讨论的情况，但安全研究人员已经确定了几个其他针对比特币的潜在攻击载体。*See* Bonneau et al, supra note 55, at 7-9.

难以攻破的倚仗。即便在今天,想要攻破比特币系统,也需要数百台运转速度最快的超级计算机一刻不停地工作才能实现。

尽管如此,由于大多数挖矿行为是通过多个参与者共同运作的矿池进行的,某一矿池能够聚集过半的挖矿能力并非痴人说梦。〔120〕51%攻击发生的风险与挖矿网络能力成反比。〔121〕比特币价格下跌,矿工激励减少时,或者算法自动减少奖励,减慢系统新货币注入时,就可能出现上述攻击。〔122〕其他区块链平台(例如瑞波)使用无挖矿奖励的共识方法,而以太坊则计划转换其共识方法,改为使用权益证明。〔123〕然而,这些技术自身都有局限性,实际适用也不如比特币广泛。许可区块链为其网络的参与者增加中心化信任代码,因此无须担心 51%攻击,中心化系统的传统信息安全问题才是其需要担心的问题。

系统的安全和稳定级别视具体情况而定。与处理小额客户交易的商人相比,银行会更加关注特定风险。区块链上的医疗记录与钻石的供应链记录具有不同的风险特征。这种变化并非区块链独有,现有中心化系统的信任和安全也存在这种变化。虽然分布式分类账具有新颖性,但甄选出恰当的安全模式还需要一些时间。

2.信任智能合约

实施交易的智能合约是第二层保障。〔124〕智能合约和其他软件代码一样,也存在误差和安全漏洞。事实上,久负盛名的以太坊智能合约中就存在明显漏洞。〔125〕由于区块链直接运作价值或财产权利,智能合约存在误差或安全漏洞极其危险。以在区块链上运行软件替代人工执行协议面临着诸多实际限制。计划往往赶不上变化。

引言中提及 DAO 的崩溃印证了这一漏洞。〔126〕依照 DAO 的规定,窃取资金的交易属于有效的智能合约,所以此类交易与其他交易一样,可以无条件执行。以太坊不得不使用"硬分叉"手段来追回被盗取的以太币。〔127〕硬分叉创制出两条互斥链。〔128〕尽管大多数矿工使用新的软件且并无意外发生,但这一举措并非无可争议。〔129〕这意味着以太坊的交易并非真正不可逆或者完全不受中心化干预的影响。同时,若政府或其他中央权威机构开始关注分布式分类账储存的记录,会造成什么后果也是需要考虑的问题。〔130〕

〔120〕*See* Jon Matonis, *The Bitcoin Mining Arms Race: GHash.io and the 51% Issue*, CoinDesk (July 17, 2014, 16:20 BST), http://www.coindesk.com/bitcoin-mining-detente- ghash-io-51-issue/.

〔121〕更一般地说,公共链必须保持足够的规模和网络效应才能保持可行性。*See* Fairfield, *supra* note 42, at 823-24.

〔122〕*See* Fredrick Reese, *As Bitcoin Halving Approaches, 51% Attack Question Resurfaces*, COINDESK (July 6, 2016, 12:50 BST), http://www.coindesk.com/ahead-bitcoin-halving-51- attack-risks-reappear/ (描述了 2016 年 7 月比特币数量减半后对 51%攻击的担忧).伴随着比特币日渐增加的稀缺性,其价格在这些减半点附近趋于增加,但即便如此,仍无法保持平衡。 其他区块链不一定使用减半机制,但所有工作人员在加密货币价格下跌时都会面临激励问题。

〔123〕*See* Vlad Zamfir, *Introducing Casper "the Friendly Ghost,"* ETHEREUM BLOG (Aug. 1, 2015), https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/.

〔124〕*See* Ari Juels, et al, The Ring of Gyges: Investigating the Future of Criminal Smart Contracts, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.

〔125〕*See* Zikai Alex Wen and Andrew Miller, *Scanning Live Ethereum Contracts for the "Unchecked-Send" Bug*, Hacking, Distributed (June 16, 2016, 1:15PM), http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/.

〔126〕Christoph Jentzsch, Decentralized Autonomous Organization to Automate Governance, https://download.slock.it/public/DAO/WhitePaper.pdf (last visited July 5, 2016).

〔127〕*See* Paul Vigna, *Ethereum Gets Its Hard Fork, and the 'Truth' Gets Tested*, WALL. ST.J. MONEYBEAT BLOG (Jul 20,2016 10:56 am ET), http://blogs.wsj.com/moneybeat/2016/07/20/ethereum-gets-its-hard-fork-and-the-truth-gets- tested/.

〔128〕即使矿工可能使用相同的协议,一条链上的矿工也无法识别其他客户挖掘区块的有效性,反之亦然。*See* Bonneau et al, *supra* note 55, at 10.

〔129〕*See* Stan Higgins, *Will Ethereum Hard Fork? DAO Attack Prompts Heated Debate*, COINDESK (June 17, 2016, 16:18 BST), http://www.coindesk.com/will-ethereum-hard-fork/; Michael del Castillo *Specter of Ethereum Hard Fork Worries Australian Banking Group*, COINDESK (June 29, 2016, 17:10 BST), http://www.coindesk.com/spectre-ethereum-hardfork- worries-anz-banking-group/.

〔130〕正如比特币一样,以太坊是一个公共区块链。 由于只有已经识别的用户允许访问,许可区块链不提供相同的不干涉保证。

有人提出分叉区块链可能会逐渐消失。这一假设并未实现。有一小部分矿工(且数量日益增多)仍在运行旧版软件,[131]明确表达了对以太坊基金会破坏分类账恒定性的不满。一部分开发者同意以"以太坊经典"(EthereumClassic)(简称 ETC)之名管理新的软件。以太坊核心开发者皮特·茨拉吉(Pete Szilagyi)对这一实践进行深刻总结,指出"去中心化组织对智能合约编写的投入远超我们的预期……"。[132]

DAO 攻击事件的影响余波犹在。2017 年 5 月,加拿大最大的加密货币交易所 QuadrigaCX 宣布,其损失了价值超过 1400 万美元的以太币。[133]其间不存在任何不当行为,丢失的以太币也并未消失,但由于智能合约出错,这笔以太币永远也追不回来。事实证明是硬分叉后用于分离以太坊和以太坊经典的余额的代码出现了错误。[134]密码恒定是保证区块链系统可信度的有力武器,但同样会造成代码难以解决的问题。

3.信任边缘服务

即使价值存储于去中心化系统,我们通常是通过中心化边缘服务获取价值。理论上来讲,在诸如比特币或以太坊的公共网络上,任何人均可获得所在区块链的副本,并运行一个完整节点。但在实践中,严苛的技术和硬件要求往往令普通用户望而却步。几乎所有消费者都会使用钱包服务(例如 Coinbase 或 Xapo)。用户必须像信任银行一样信任钱包服务。钱包服务提供商为其客户储存私钥,客户可以使用标准的用户名和密码获取其加密货币。然而,若钱包服务提供商受到黑客攻击,密钥的安全就难以保障。加密货币毕竟是新兴产物,还有许多不足之处。其正如尼克·萨博在推文中所说:"比特币本身是世上安全性最高的金融网络,但其中心化外围公司却非常不安全。"[135]

加密货币和美元或其他政府支持的法定货币的兑换中存在明显的漏洞。在工作量证明系统(例如比特币)中,想要获得加密货币,只能通过挖矿或者与他人交换。大多数用户并非矿工,所以某些时候他们需要购买比特币。交易所开展不同加密货币和美元或其他法定货币之间的交易。但很遗憾,有些时候交易所难以完成上述交易。

2014 年,黑客从最负盛名的比特币交易所 Mt. Gox 窃取了价值 4 亿美元的比特币,Mt. Gox 随之倒闭。[136]2016 年,另一家主要交易所 Bitfinex 也遭到黑客攻击,被窃走价值 7000 万美元的货币。[137]据统计,至少有 15 起加密货币盗窃事件,其中失窃额最低为 100 万美元,总失窃额超过 6 亿美元。[138]尽管有人提出,加密货币交易所应获许可方可营业(例如纽约的比特币牌照),但加密货币市场的全球性决定了大多数交易所如今都还处于无监管状态。[139]

〔131〕*See* Vigna, *supra* note 30.

〔132〕*See* Peter Szilagyi, *DAO Wars: Your Voice on the Soft-Fork Dilemma*, ETHEREUM BLOG (June 24, 2016), https://blog.ethereum.org/2016/06/24/dao-wars-youre-voice-soft-fork- dilemma/.

〔133〕*See* Stan Higgins, *Ethereum Client Update Issue Costs Cryptocurrency Exchange $14 Million*, COINDESK (June 2, 2017, 19:00 UTC), https://www.coindesk.com/ethereum-client- exchange-14-million/.

〔134〕*See id.*

〔135〕Nick Szabo (@NickSzabo4), Twitter (June 17, 2017, 9:04pm), https://twitter.com/NickSzabo4/status/876244539211735041.

〔136〕*See* Amir Mizroch, *Large Bitcoin Exchange Halts Trading After Hack*, WALL ST. J.:DIGITS BLOG (Jan. 6, 2015, 4:13 AM), http://blogs.wsj.com/digits/2015/01/06/large-bitcoin- exchange-haltstrading-after-hack; Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED.COM (March 3, 2014), http://www.wired.com/2014/03/bitcoin- exchange/.

〔137〕Josh Horwitz, *The $65 Million Bitfinex Hack Shows That It Is Impossible to Tell a Good Bitcoin Company From a Bad One*, QUARTZ (August 9, 2016), https://qz.com/753958/the-65-million-bitfinex-hack-shows-that-it-is-impossible-to-tell-a-good-bitcoin-company-from-a-bad-one/.

〔138〕作者的分析基于 Michael Matthews 的 List of Bitcoin Hacks (2012-2016), Steemit, https://steemit.com/bitcoin/@michaelmatthews/list-of-bitcoin-hacks-2012-2016 and other sources.

〔139〕这种情况可能会改变。作为最大交易所之一的 Bitfinex 于 2017 年 8 月宣布,它将停止为美国客户提供服务,因为美国证券交易委员会表明,若未在发行时妥善地登记为证券,Bitfinex 可能需要为其交易的代币承担责任。*See* Wolfie Zhao, *Bitfinex to Bar US Customers from Exchange Trading*, COINDESK (Aug.11,2017,23:20UTC), https://www.coindesk.com/bitfinex-suspends-sale-select-ico-tokens-citing-sec- concerns/.

边缘服务提供商同样可以决定是否对交易进行监督。分类账对比特币交易的标的并无任何甄选标准,无论以比特币购买毒品、进行赌博、买凶杀人还是订购披萨,其处置并无任何差别。交易不通过任何银行或支付平台,政府难以施压阻止。但若用户通过边缘服务提供商进行交易,则会受到法律实施的制约。然而,考虑到服务提供商所在地不定及提供商可能需要对其用户身份保密,实施监管还是存在一定难度。如"丝绸之路"骇客追缉令以及类似的法律实施举措所示,上述事实并非完全不可能。〔140〕

4.信任代币发行人

最后一个漏洞源与区块链服务项目有关。若这些服务项目为中心化系统,必定存在与交易所或其他边缘服务项目类似的问题。若为去中心化系统,就会以有漏洞的智能合约为运作基础。许多区块链服务项目会通过直接向用户发行自有加密货币添加新的元素。销售此类代币会引发更深层次的问题。

公司可以向公众销售股票,为公司运营融资。同理,分布式分类账网络或 DApps 也可以销售加密货币代币。类似于股票的首次公开发行(IPO),以上代币的销售通常被称为首次代币发行(简称 ICO)。代币授予的权利取决于对应智能合约。〔141〕万事达币(Mastercoin)是在比特币网络制造特定专用"彩色"代币的系统,是第一个 ICO 项目。其 2013 年进行的 ICO 生成了 500 万美元的比特币。2014 年(首个以太币区块开采完成前一年),以太坊随之进行了 ICO,募集约 1800 万美元的比特币。2017 年,随着比特币价格暴涨,出现一股 ICO 狂潮,募集到近 20 亿美元的资金。〔142〕

代币销售为规避传统风险投资模式限制的创新科技提供了新的融资手段,同时也是欺诈民众财富的完美方法。如今代币的购买者通常只为区块链项目投入资金,但并不会收到任何收益保证,对于投资风险的了解也十分有限。其投资的项目可能是骗局。发起项目的团队可能心有余而力不足,难以开发出其构想的应用。相对于开发团队或其合伙人,发行条款可能对购买者并不公平。开发出的应用也可能难以吸引用户,因此造成代币价值的下降。

以上风险与引起《1933 年证券法》和《1934 年证券交易法》制定颁布的风险有诸多共同之处。〔143〕美国证券交易委员会(SEC)规则要求所有证券发行必须登记(继而对详细披露和防欺诈提出要求)或者适用特别豁免。但几乎所有的 ICO 项目都没有遵守上述规则。

证券监管的基本原则就是披露。投资有风险,任何人均无权利保护错误的投资决策。然而,若无监管,投资者(尤其是小额投资者)和投资发起人之间存在严重的信息不对等。代币销售代表了一种以世界范围内小额投资者为目标的"购者自慎"证券发行的大胆尝试。〔144〕考虑到区块链技术的不确定性和技术复杂性,即便项目发起人进行了广泛的财务信息披露,大多数投资者仍可能对其投资的项目一知半解。因此,投资者很可能任由发行人和投资发起人为所欲为。权力滥用如此严重,项目会成为骗局也是难以避免的。〔145〕

ICO 可能被滥用并不等于整个项目都会被禁止,或者所有此类发行活动都必须符合美国证券法

〔140〕*See supra* note 20 and accompanying text.

〔141〕合约通常不会提供与股票相关的公司实体的股权。代币持有者拥有的是网络价值的一部分,而不是一项资产的正式债权。

〔142〕*See supra* note 10.

〔143〕Securities Act of 1933, Pub. L. No. 73–22, 48 Stat. 74 (1933) (codified as amended at 15 U.S.C. § § 77a–77aa (1982 & Supp. IV 1986)); Securities Exchange Act of 1934, Pub. L. No. 73–291, 48 Stat. 881 (1934) (codified as amended at 15 U.S.C. § § 78a–78kk (1982 & Supp. IV 1986)).

〔144〕美国证券法只适用于证券销售或出售给美国公民的情况。但是,大多数其他主要司法管辖区都有类似的披露义务。正如美国证券交易委员会在其关于 DAO 代币发行的调查报告中所确认的,一家向美国人出售代币的外国实体甚至虚拟组织仍然需要遵守其规则。*See* Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (July 25, 2017), https://www.sec.gov/litigation/investreport/34–81207.pdf [SEC DAO Investigation].

〔145〕*See* David Z. Morris, *The Rise of Cryptocurrency Ponzi Schemes*, ATLANTIC (May 31, 2017), https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency–ponzi– schemes/528624/.

的严格规定。首先,并非所有代币发行都必须是证券。SEC 近期所作调查得出结论,The DAO 的代币应被归类为证券,因此需遵守 SEC 关于公开发行的规定。〔146〕但其并未认定所有代币为证券。全世界的监管者需要对代币发行项目的区分方式加以考量,帮助投资者剔除无意义的创新,保护其利益。问题的关键在于,如果不这样做,投资者就会受到伤害。ICO 失败会破坏市场的整体信心。虽然区块链有效执行了去中心化安全模型,但这一事实并不能消除对法律和监管介入的需求。

(二)代码和法律

1.“众聚之地,非王之土”

20 世纪 90 年代末,主流观点往往将互联网视为一种以去中心化方式破坏监管的科技。电子前沿基金会(Electronic Frontier Foundation)的创始人约翰·佩里·巴洛(John Perry Barlow)在其提出的《1996 年网络空间独立宣言》中称“在我们聚集的地方并无统治权”,且并不“存在令我们害怕的执行手段”。〔147〕这一观点抓住了网络解放运动的精神,该运动的参与者不仅包括老派的国家权力怀疑论者,还包括专注创新的开发者以及法律专家。学者认为网络社区挣脱了区域统治的桎梏。〔148〕有些网络积极分子甚至主张公海内废弃的英国海军平台为西兰公国的独立领土,坚信其可以完全不受法律限制约束运行互联网服务器。〔149〕

网络空间不受监管的观点与冷硬的现实限制相契合。正如杰克·戈德史密斯(Jack Goldsmith)和吴修铭(Tim Wu)在其 2006 年著作《谁控制了互联网》一书中解释道,世界各国政府能够将其意志强加于网络活动。〔150〕类似西兰公国的乌托邦式倡议出师未捷身先死,失败的原因往往是内讧。〔151〕中国建立了“防火长城”,检查国土内外的网络流量。〔152〕而地理定位技术则令法院能够对涉及其辖区居民的活动施以惩罚。〔153〕无论是通过点对点技术来拖延版权执法行为或在赌博合法化岛屿开展线上赌博服务,规避法律制度的活动屡次被禁止。威权体制发现可以利用网络本身作为监督和镇压的手段。〔154〕

互联网的确广而新。但法律体系能够容纳吸收互联网,就像吸收印刷机之后的每项技术一样。事实证明,虽然网络空间是虚无缥缈的,但提供网络服务的人、公司和系统却是实际存在的。从控制比特流的网络服务和托管服务提供商到控制资金流量的金融服务公司,存在多个控制点,监管者可以任意选择对在线活动进行管控。〔155〕互联网是一个受监管的空间。〔156〕当然,这并不意味着其监管方式与其他空间相同,也不意味着线上交易的监管方式与线下交易相同。网络监管的适用性是一个全球性问题,对这一问题的探索跨越了 20 年历程,且离胜利遥遥无期。但有一点毋庸置疑,即网络与监管并不矛盾。

区块链重燃网络解放之火。有关区块链和法律的讨论有两种构建方式:能否对相关技术进行法律和行政监督?是否应该对其进行法律和行政监督?许多区块链开发者和拥护者(尤其是在比特币初生阶段就开展研究的开发者和拥护者)对以上两个问题都作出了肯定的回答。他们指出,加密货币旨在解决价值导向交易的政府监督问题。中本聪的突破性进展旨在创造脱离监管桎梏的财富。就此而

〔146〕*See* SEC DAO Investigation, *supra note* 144. 美国证券交易委员会得出结论,DAO 是一种未经授权的未经登记的证券发行,但“基于委员会此时已知晓的行为和活动”选择不实施制裁。Id. at 1. 这显然表明,由于硬分叉,所有投资者都收回了他们的钱,而 DAO 随后关闭。

〔147〕John Perry Barlow, A Declaration of the Independence of Cyberspace, https://www.eff.org/cyberspace-independence.

〔148〕*See* David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

〔149〕*See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).

〔150〕*See id.*

〔151〕*See id.*

〔152〕*See id.*

〔153〕*See id.*

〔154〕*See EVGENY MOROZOV, THE NET DELUSION (2011).*

〔155〕*See* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2002).

〔156〕对此,相信细心的读者已从前述劳伦斯·莱西格的著作中得以窥探。*See* Lessig, *supra* note 22.

言,共识计算的去中心化结构就是一道阻隔政府干预的防火墙。区块链不仅恒定不变,还具有"抗审查性"。没有哪个上级机关能够要求区块链做任何事,也不能支配网络。监管和区块链是相互对立的。

分布式分类账的支持者对这一观点深信不疑。莱特和德·菲利比将区块链的"Lex Crptographica"与福特汉姆大学法学院教授乔尔·雷登伯格(Joel Reidenberg)在1997年发表的文章中描述的软件代码的"Lex Informatica"直接联系起来。〔157〕他们指出,自动执行的智能合约和去中心化自治组织在私人法律系统的实施过程中,并不以领土国家为限,这一点与比特币创造私有全球化货币的方式几乎一样。

过去20年的经验证明,政府和强大的私立机构很难被架空。〔158〕只要他们打定主意要监管线上活动,就会想方设法达成目的。区块链活动同样适用这一模式:只要有足够多的利益,政府便不吝于插手。即使交易是完全数字化、点对点、跨境且加密保护的,网络上供应商的身份也能够被确认,且会受区域法律义务的约束。〔159〕此外,除了非法活动或需要严密保护的活动之外,在现行法律系统正常运转的情况下,缺乏足够的激励推动大多数用户采用定制法律系统。〔160〕去中心化组织的创造者发现,取代法律并不像想象中那样简单。

莱特和德·菲利比承认这一事实。他们提出了更为中庸的主张,即通过与其他监管模式相关的代码,区块链或许能够扩宽监管的范围。〔161〕但这一主张应由持反对观点的人加以印证。值得注意的是,虽然以中本聪共识为基础的分布式分类账是新概念,智能合约和数字货币却不是。20世纪90年代早期,尼克·萨博提出了智能合约私法监管机制,但加密型私法并未普及开来。

原因之一,是恒定共识并无任何折衷办法。OpenBazaar是一个类似于易趣的分布式加密货币网上商城,其创始人之一指出:"若允许用户对传统法庭和法律负责,就相当于打开了潘多拉魔盒,政府可以自主规定'交易欺骗行为'的界限,以此进行干预,为审查制度大开方便之门……"〔162〕

许多人鼓励一些意见分子利用区块链技术来发布非法民主宣言。但区块链技术的作用远不止此。在真正去中心化网络中,无论是向已知的恐怖组织转移资金、贩卖儿童作为现代奴隶还是洗黑钱,任何交易都是没有限制的。完全自由的极限便是无政府,即托马斯·霍布斯所指的各自为战、相互倾轧。〔163〕

Augur预测市场平台提出了这一难题。〔164〕唐(Don)和亚历克斯·泰普斯科特(Alex Tapscott)在其畅销书《区块链革命》中对Augur的潜力大加吹捧。他们发现,"暗杀市场和恐怖主义期货"等问题是中心化预测市场(例如Intrade)关闭的部分原因。随后犀利地指出,这些对于区块链预测市场来说不

〔157〕*See* Wright and De Filippi, supra note 23 at 44–47; Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEXAS L. REV. 553 (1997). 雷登伯格提出的"Lex Informatica"与莱西格通过软件架构进行监管的"West Coast code"是基本相关的。

〔158〕*See* generally Kevin Werbach, *The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy*, __ Fla. L. Rev. __ (forthcoming 2017)(详细说明了不受监管数字空间的愿景如何失败);Goldsmith & Wu, supra note 150(显示政府如何成功地对线上活动实施控制)。

〔159〕*See* Goldsmith & Wu, *supra* note 150. 若想对此进一步验证,请参考Grokster、Kazaa和Streamcast的命运,当美国最高法院宣布他们应对其共同侵犯版权的行为承担责任时,这些分散的文件共享服务则被关闭。*See* MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). 法院不能完全阻止开放源代码点对点软件的传播或使用,但他们可向利用该软件赚钱的公司强行施加责任。用户群的边缘活动与可向主流扩展的重要市场之间存在重要差异。

〔160〕乔什·费尔菲尔德提出一个极具吸引力的观点,即智能合约可用来与在线网站协商服务条款,借此使权力重返用户,而该观点也存在类似问题。*See* Josh Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 36 (2014), http://scholarlycommons.law.wlu.edu/wlulronline/ vol71/iss2/3. 目前尚不清楚服务提供者为何会作出让步。

〔161〕Tapscott & Tapscott, *supra* note 37, at 84.

〔162〕Dionysis Zindros, Trust is Risk: A Decentralized Trust System, OpenBazaar, https://www.openbazaar.org/blog/trust-is-risk-a-decentralized-trust-system/.

〔163〕THOMAS HOBBES, LEVIATHAN, OR, THE MATTER, FORME, & POWER OF A COMMON WEALTH ECCLESIASTICALL AND CIVILL (1676).

〔164〕Pete Rizzo, *Augur Bets on Bright Future for Blockchain Prediction Markets*, CoinDesk (March 1, 2015, 13:30 BST), http://www.coindesk.com/augur-future-blockchain-predictionmarket/.

成问题，“Augur 对犯罪行为实施零容忍政策，因而可以解决不道德合约的问题”。〔165〕

但这完全是避重就轻。管辖各合约方、开发者和预测市场其他参与者的法律相互冲突时，应该如何定义犯罪行为？判定何为不道德更是难上加难。在这种情况下，零容忍又意味着什么？什么问题会上传到预测市场，Augur 的开发者根本无法控制。在脸书或 Reddit 上，管理员可以删除用户上传的非法的、攻击性或骚扰性的资料。但在 Augur 这样的分布式平台上，此举并不可行。若有人在 Augur 上发布了非法合同（例如暗杀合同），谁能阻止这种行为呢？类似项目的创新范围似乎必然会与合法公共政策考量相冲突。

2.监管争论

区块链系统相关监管争论已经产生。广义而言，争论主要围绕以下三点展开：不合法性、分类以及法律效力。

首先，区块链系统的不合法性涉及利用加密货币违法或通过黑客行为或类似手段窃取加密货币。比特币可以用来购买毒品，这一事实本身并不会引起加密货币的法律问题，因为人民币或金条也能实现相同的目的。问题的关键在于化名或匿名的私有去中心化货币会大大降低实施此类违法行为的难度，且行为人无需为此承担任何责任。与恐惧相反，大多数主要西方政府并未因此对加密货币加以禁止。反而是认识到比特币和类似货币的基本合法性之后，大多数国家选择了禁止。这并不意味着在受监管的银行体系内或者有其他特定用途的情况下就是合法的，只是以加密货币进行交易这一行为本身并不被禁止。

代码既增加了审查和干预的难度，同时也为恐怖融资和勒索软件提供便利，应当如何处理代码则是一个开放性问题。另一相关问题是：在创制去中心化数字不记名票据的同时，代码也为（内部和外部）窃贼创造了一个诱人目标。这两个问题（分别在丝绸之路和 Mt. Gox 有所体现）是比特币初期至今最突出的法律问题。

其次，区块链系统的分类涉及的活动基本合法，但不符合非区块链对等系统相关法律的要求。加密货币交易所或矿工能否是货币转让代理人或依照美国州或联邦法律建立的银行？代币发行能否是依照 SEC 规则进行的证券发行？负责发行活动的人是不是投资经理？加密货币交易所是不是依照商品期货交易委员会（CFTC）监管要求建立的衍生品市场？受监管金融机构遵守反洗钱 / 了解客户（AML/KYC）规则的，是否应当要求加密货币服务提供商获取有关其客户及交易目的地的验证信息？因加密货币升值带来的利益是否应当像资产和货币一样缴纳所得税？类似的问题还有很多。

最后，其他法律结构是否认可分布式分类账？各国逐渐倾向于将区块链信息当作传统记录进行处理。特拉华州通过立法，授予分布式分类账政府记录和监管功能，例如追踪公司股票和优先权的情况。〔166〕亚利桑那州通过一项法案，主张区块链数字签名具有法律效力。〔167〕弗蒙特州允许区块链信息作为证物呈堂。〔168〕至于分类问题，还有许多具体问题需要考虑，各司法管辖区必须行动起来。

3.不公开合约

智能合约是区块链系统难以切断与法律联系的另一领域。智能合约好像是法律实施的混乱程序更优的替代品。若各方能够就合约条款达成合意且分布式机器网络每次都能完美执行协议，何必依赖效率低下、可能不准确或有偏见且管辖受限的法院呢？区块链的拥护者普遍坚持这一观点。〔169〕此处

〔165〕Tapscott & Tapscott, *supra* note 37, at 84.

〔166〕*See* Jeff John Roberts, *Companies Can Put Shareholders on a Blockchain Starting Today*, FORTUNE (Aug. 1, 2017), http://fortune.com/2017/08/01/blockchain-shareholders-law/.

〔167〕*See* Stan Higgins, *Arizona Governor Signs Blockchain Bill into Law*, COINDESK (March 31, 2017, 16:08 UTC), https://www.coindesk.com/arizona-governor-signs-blockchain-bill-law/.

〔168〕http://legislature.vermont.gov/statutes/section/12/081/01913.

〔169〕*See, e.g.*, Tapscott & Tapscott, *supra* note 37, at 109（“通过智能合约……公司可以依靠完全的透明度来规划关系……总之，无论喜欢与否，他们开展业务必须兼顾他方利益。这是平台的要求”）；Cassano, *supra* note 76（“这些项目可能会在某天将律师取代……”）.Andrew Keys, *Memo from Davos: We Have a Trust Problem. Personal Responsibility and Ethereum are the Solutions*, CONSENSYS BLOG (Jan. 19, 2017), https://media.consensys.net/memo-from-davos-we-have-a-trust-problem-personal-responsibility-and-ethereum-are-the-solutions-19d1104946d8#.c46zvkcks（“现仍尚处早期，律师、审计师和监管机构必然需要去学习、教育和促进智能合约，但这一过程将变得更加自动化，中介机构将被摒弃，信任成本将会骤降”）.

的推理漏洞在于未能区分合同履行和执行。实施协议的具体步骤并非难事,在现实中也不稀奇。在没有人为干涉的情况下,每天有数十亿美元的衍生品交易自动达成。计算机按照合同条款进行编程,并在特定情形出现时自动履行交易。

针对"可计算合约"(法学教授和软件工程师哈利·舍尔顿提出的概念),区别在于协议可以自动履行但不能自动执行。[170]相关方可以在履行前修改协议,随后法院能够撤销该修订。智能合约放弃对保存分类账的去中心化网络的所有权力,自动开展合约执行。[171]代码之外的任何内容都仅具有解释功能。或引用去中心化组织服务条款的内容,其"仅具教育目的"。[172]

自动化合约执行不会像自动执行那样简单,将法律系统从合约程序中剔除必定会带来巨大的潜在利益。不可阻挡的合约仅靠糊涂法官、腐败地方官、贪婪政府或诡诈相对方一时心血来潮是难以维持的。把律师踢出合约执行闭环的潜在效能和自动化收益相当可观。但这一程序同样导致了 DAO 的灾难性失败。

无论计算速度有多快,计算机终究不能取代人类。智能合约也一样。[173]代码的确无法有效解释诸如"合理"或"最大努力"之类的术语。而且有些时候以当事方的意图理解合约含义会比照本宣科、以合约条款的字面意思为准更加贴切。The DAO 就是典型的例子。试图窃取资金的攻击者和通过硬分叉夺回被盗资金的矿工,两者唯一的区别就是动机不同。[174]而电脑根本不能对动机进行评估。

即使智能合约充分执行了协议,只要当事方对结果不满,还是会诉诸诉讼。[175]若法官相信确有不公正或法律上可辨伤害存在,就不会袖手旁观,不会任由分布式分类账做主。化名或匿名相对方的身份确认以及针对其他国家行为主体提起诉讼的确面临许多实际困难。就前者而言,无论能否胜诉,当事方总有可以起诉的对象。如果 DAO 的出资人未能通过以太坊硬分叉追回资金,有些人毫无疑问会起诉 Slock.it(Dapp 的开发者)和以太坊基金会。就后者而言,跨境合约纠纷是跨国公司现代商务的重要部分。智能合约的当事人中,必定有人会拒绝出庭,但大公司往往不会拒绝出庭。管辖权和法律适用的确难度很大,但并非无解之局。

(三)监管和创新

1.加密服务提供商的分类

监管往往被看作是创新的对立面。对许多人而言,政府参与加密货币和区块链系统的开发势必会拖慢和腐蚀新系统的开发。若政府只在民众无法互信且对托马斯·霍布斯所提"君主专制国家"毫不担心的情况下才会存在,那么中本聪就能解决监管和创新的对立问题。

然而,我们同样有理由质疑传统的网络自由主义观点。互联网的监管是其广泛普及的重要举措之一。[176]早期"有效的"许多举措其实是线上社区小范围试点成果的推广。随着互联网越来越社会化,其和实体社区一样,面临着同样的政治和经济挑战。例如,20 世纪 90 年代末,微软利用其垄断权力威胁互联网初创公司,美国政府就通过反垄断执法对其进行干预和约束。[177]此外,政府的存在是为了监督滥用行为,这一认知有利于提升虚拟交易活动中的信任。互联网的支持者开始呼吁政府进行干预,实施网络中立规则并对隐私进行保护。[178]

〔170〕*See* Harry Surden, *Computable Contracts*, 46 U.C. DAVIS L. REV. 629 (2012).

〔171〕*See* Werbach and Cornell, *supra* note 25.

〔172〕The DAO 的服务条款页面已不再可用。对于同一引文,*see* Joel Ditz, *DAOs, Hacks and the Law*, Medium (June 17, 2016), https://medium.com/@Swarm/daos-hacks-and-the-law-eb6a33808e3e.

〔173〕Werbach & Cornell, *supra* note 25.

〔174〕*See id.*

〔175〕*See id.*

〔176〕*See* Werbach, *supra* note 158.

〔177〕*See id.*

〔178〕*See id.*

分布式分类账科技也存在类似情况。随着罗斯·乌尔布里奇锒铛入狱,区块链活动不受法律制约的观点不攻自破。亚历山大·温尼克(Alexander Vinnik)(Mt. Gox 数十亿美元失窃案的主谋,通过交易所和混合服务器掩盖行径,令追踪比特币交易难上加难)也难逃被捕的命运。〔179〕尤其是伴随许可分类账和以公共分类账为基础的企业级系统的兴起,监管能够促进区块链的发展获得普遍认可。这并不是说形势一片大好。互联网为政府发挥主观能动性和新兴产业积极负责提供了正面榜样。〔180〕虽然也有很多反面教材,但有足够的实例证明,监管者和被监管者相互配合,是可以促进新兴产业成长和创新的。但即便如此,也不能保证这一结论同样适用于区块链。

和违法黑客、侵权内容分销商和身份窃贼经常访问非区块链"暗"网一样,类似丝绸之路的违法加密货币市场也未停止运转,但这种鬼鬼祟祟的行为规模有限。大多数人并不会在线上购买毒品或花钱获取流媒体服务。区块链为法律实施带来了新的挑战,但其并非特例。互联网、20 世纪 90 年代初期加密技术的发展、20 世纪 80 年代私人电脑的普及等都曾挑战法律实施。相关的例子不胜枚举。当今世界的数字化技术是一把"双刃剑",亦正亦邪。区块链虽然为其开启了新篇章,但并不能改变其原有的力量均势。

诚然,科技的监管和许可用途的区分还存在许多重要问题亟待解决。一旦有可趁之机,罪犯和恐怖主义者会挖空心思地榨取区块链利益,就像盘剥其他科技一样。政府会反应过度,提出"伤敌一千,自损八百"的规则,控制非法行为的同时,对合法经营造成损害。以上叙述旨在揭示,这些老生常谈的问题不应被视为区块链与合法性相互对立的证据。真正有趣的问题是,当新兴科技并不违反法律时,如何区分科技的监管和许可用途。通过提出高效新颖的信任和合规机制,区块链怎样才能取代现有的法律制度?在什么情况下,现有的法律制度才算过度约束区块链创新?

如前所述,大多数监管都是一种分类实践。规则建立状态分类,监管者对符合分类的人进行监管。有些时候,分类是清晰明确的。威瑞森电信(Verizon)和美国电话公司(AT&T)对完善固话服务并无争议,依据《1934 年通信法案》,两家公司被归类为"电信运营商"。〔181〕但有些时候,分类并非易事。康卡斯特(Comcast)过去不提供电话服务,现在使用互联网技术在特定包交换数据网上提供相关服务;沃纳奇(Vonage)自有网络设施,向宽带用户提供语音电话服务应用;亚马逊在其 Echo 个人助理设备支持语音信息。这些公司是否都符合"电信运营商"这一分类呢?

问题的答案很简单,相关的服务只要外表类似、功能相同就应归入相应分类进行监管。网络电话的实际定义经历了十多年的激烈争论。〔182〕这并不是一件坏事。联邦通信委员会(FCC)担心预置的过度监管会抑制创新。〔183〕在 20 世纪 90 年代,想要快刀斩乱麻,干脆地解决分类争议几乎不可能,因为当时的技术还不成熟,且实施范围有限。

当下的监管者在划分加密服务提供商的类别时遇到了同样的问题。〔184〕2015 年,金融犯罪执法网(FinCEN)(美国财政部的金融犯罪执法办公室)向瑞波提起民事诉讼。〔185〕瑞波使用区块链来大幅降

〔179〕*See* Samuel Gibbs, "*Criminal Mastermind*" *of $4bn Bitcoin Laundering Scheme Arrested*, GUARDIAN (July 27, 2017, 5:10 EDT), https://www.theguardian.com/technology/2017/jul/27/russian-criminal-mastermind-4bn-bitcoin-laundering-scheme-arrested-mt-gox-exchange-alexander-vinnik.

〔180〕*See* Werbach, *supra* note 158; Kevin Werbach, *The Federal Computer Commission*, 84 N.C. L. REV. 1 (2005).

〔181〕47 U.S.C. 153(51).

〔182〕*See* Kevin Werbach, *No Dialtone: The End of the Public Switched Telephone Network*, 66 Fed. Comm. LJ 203 (2013).

〔183〕*See id.*

〔184〕*See* Camila Russo, *Ethereum Co-Founder Says Crypto Coin Market Is a Time-Bomb*, BLOOMBERG TECHNOLOGY (July 18, 2017, 1:40pm EDT), https://www.bloomberg.com/news/articles/2017-07-18/ethereum-co-founder-says-crypto-coinmarket-is-ticking-time-bomb(引用瑞波首席执行官布拉德·加林豪斯的话,即:"如果它的言行与一只鸭子无异,那么美国证券交易委员会将会说它就是一只鸭子").

〔185〕*See* Sarah Todd, *Fincen Fines Ripple Labs Over AML, Says Firm 'Enhancing' Protocol*, AMER. BANKER (May 5, 2015, 7:41pm EDT), https://www.americanbanker.com/news/fincen-fines-ripple-labs-over-aml-says-firm-enhancing-protocol.

低国际转账汇款的交易费,年市场总值达到数十亿美元。FinCEN 起诉的原因是瑞波在此过程中并未登记成为受监管的资金服务企业。〔186〕处理转账业务无可厚非,问题是在此过程中不承担该行业其他参与者负有的义务。尤其是瑞波未能遵守反洗钱和"了解客户"(AML/KYC)规则。以上规则旨在阻止罪犯和恐怖主义者利用银行系统支持其活动。就 FinCEN 提起的诉讼,瑞波同意缴纳 450,000 美元的罚款,并承诺建立 AML/KYC 合规制度。〔187〕

瑞波处罚可谓是加密货币产业的转折点。比特币是在分布式网络实施的协议,而瑞波是一家以营利为目的的公司。其经营模式由其与全世界金融机构发展合作关系的能力决定,这样才能进行各地货币与瑞波币(XPR)的交易。对瑞波而言,FinCEN 的处罚意义重大。AML/KYC 程序通常要求金融服务经营者对实际身份文件(例如护照)进行验证,并与个人黑名单交叉对比,这一程序可能非常麻烦,尤其对于快速发展和高度信息化的服务提供者而言。

有些公司将 FinCEN 案视为美国不欢迎加密货币公司的信号。处罚决定作出 10 日后,风险投资型比特币初创公司 Xapo 就将其总部从加利福尼亚迁至瑞士。〔188〕几个月之后,纽约州金融服务局要求在该州营业的虚拟货币企业获取"比特币牌照"(BitLicense)。〔189〕

比特币牌照背后的逻辑——加密货币交易所应与传统货币交易所同等对待——理据很充分,但实施起来却捉襟见肘。相关主体需要满足的要求过于严苛,相关规定对除保管交易所之外的很多加密货币企业进行管制,认证程序非常复杂。2017 年初至今,虽然申请比特币牌照的企业很多,该局仅签发了三张比特币牌照。〔190〕牌照的获得者(Circle、瑞波和 Coinbase)是该领域资金实力最雄厚的初创公司,继而引发这一问题:比特币牌照会排挤小规模创新企业。比特币牌照的直接后果就是,至少有 10 家比特币公司宣布其将停止在纽约的业务。〔191〕

2.管辖权竞争

互联网时代和分布式分类账时代监管争论的不同之处就是美国不再占据主导地位。如今的互联网已经高度全球化,而在 20 世纪 90 年代,互联网的使用和初创公司高度聚集于美国。相比之下,分布式分类账活动在全球范围内聚集。伦敦、柏林、瑞士和新加坡是主要枢纽,中国(主导比特币挖矿)、加拿大、韩国、爱沙尼亚和中国香港地区是重要中心。〔192〕以太坊项目负责人维塔利·布特林(Vitalik Buterin)是俄罗斯人,他在加拿大长大,是一家总部位于瑞士的基金会的负责人,现居新加坡。若其在互联网初期创业,硅谷可能会成为其目的地。

区块链开发活动的全球分布引发了各区域之间的管辖竞争。美国在早期互联网产业中的主导地位为其带来了巨大的经济利益和全球软实力方面的优势地位。各国均想成为加密经济领域的硅谷,小到直布罗陀,大到俄罗斯,均在制定新的法律体制来吸引区块链初创公司、代币发行和其他活动。瑞士楚格州地处欧洲中心,政局稳定,整体环境对加密货币公司十分友好,且制定了非常优惠的税收政策。〔193〕特拉华州是美国公司法的核心区,楚格州一直想要成为加密货币领域的特拉华州,而特拉华

〔186〕*See id.*

〔187〕*See id.*

〔188〕*See* Kia Kokalitcheva, *Switzerland is a Banking Capital. But a Bitcoin Capital?* FORTUNE TECH (May 15, 2015), http://fortune.com/2015/05/15/bitcoin-switzerland-privacy/.

〔189〕*See* Michael J. Casey, *NY Financial Regulator Lawsky Releases Final BitLicense Rules for Bitcoin Firms*, WALL. ST. J., June 3, 2015, https://www.wsj.com/articles/ny-financialregulator-lawsky-releases-final-bitlicense-rules-for-bitcoin-firms-1433345396.

〔190〕*See* Michael del Castillo, *Bitcoin Exchange Coinbase Receives New York BitLicense*, COINDESK (Jan. 17, 2017, 18:00 UTC), https://www.coindesk.com/bitcoin-exchange-coinbase-receives-bitlicense/.

〔191〕*See* Daniel Roberts, *Behind the "Exodus" of Bitcoin Startups from New York*, FORTUNE TECH (Aug. 14, 2015), http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/.

〔192〕*See* Richard Kastelein, *Global Blockchain Innovation: U.S. Lags, Europe and China Lead*, VENTUREBEAT (Apr. 16, 2017, 8:35am), https://venturebeat.com/2017/04/16/global-blockchain-innovation-u-s-lags-europe-and-china-lead/.

〔193〕*See* Kokalitcheva, *supra* note 188.

州也有相同的意图。

美国仍是区块链活动的重要推动主体之一。很大一部分比特币核心开发都发生在美国，纽约也是金融服务领域分布式分类账技术的重要中心。区块链初创公司的许多重要投资者也在美国，包括数字货币集团、区块链资本公司、安德森·霍洛维茨风投公司和联合广场投资公司。诸如 IBM、微软和普华永道之类的美国科技和服务公司也在使用分布式分类账应用方面位列前茅。美国的科技人才和科技初创公司生态系统仍然是无与伦比的。

值得重申的是，主要互联网公司并不会在西兰公国或海盗避税港落户，开发者和客户在哪里，他们就去哪里。在相关组织看来，相较于其他因素，监管并不是越少越好，而是越完善越好。对于想拥有庞大用户基础的区块链平台而言，可靠稳定的监管环境对于建立信任非常重要。同样的，即使是急于吸引某一领域（例如加密货币）创业企业的司法管辖区也不会毫无原则地妥协到底。新加坡是区块链活动的温床，一定程度上是因为其许可的监管态度。然而，2017 年 8 月，新加坡金融管理局发布一项声明，确定首次代币发行活动会受到反洗钱和恐怖主义融资规定的约束。〔194〕若发行的代币是“发行人资产或财产的所有权或担保物权的凭证”，则应归类为证券进行监管。

有些专注于创收的小国家会抱有“什么都行”的态度，但在该地进行的 ICO 活动可信度必然不高，因此难以吸引足够的资金。此外，资金输出国更不吝于行使管辖权。这也是所有公司都不在海外避税港设立的原因。

因为比特币牌照，美国在某些加密货币圈子内监管风评不佳，因而近期相关监管项目进行了相应改进。统一法律委员会制定了各州立法机构广泛适用的标准守则。2017 年，该委员会通过了一项标准加密货币法，对监管范围进行限定。〔195〕加密货币智库 Coin Center 的研究部门主任皮特·范·瓦肯伯格积极参与了该标准法的起草，并称其是“比特币和加密货币的巨大胜利”。〔196〕美国商品期货交易委员会建立了一个 LabCTFT 小组，负责研究加密货币和与该新兴产业互动。〔197〕SEC 关于首次代币发行和 The DAO 的调查报告广获好评，被赞誉谨慎详实。〔198〕

美国或任何司法管辖区能否平衡区块链系统监管方法的灵活性和保护措施尚无定论，此间争论刚刚开始。总而言之，积极尝试好过袖手旁观。

四、法律信任和区块链信任相结合

法律制度能够帮助区块链提升可信度。融合区块链分布式算法信任结构和人为诠释、国家支持

〔194〕Monetary Authority of Singapore, MAS Clarifies Regulatory Position on the Offer of Digital Tokens in Singapore （Aug. 1, 2017）, http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx.

〔195〕Peter Van Valkenburgh, The ULC's Model Act for Digital Currency Businesses Has Passed. Here's Why It's Good for Bitcoin, Coin-Center（July 19, 2017）, https://coincenter.org/entry/the-ulc-s-model-act-for-digital-currency-businesses-has-passedhere-s-why-it-s-good-for-bitcoin?mc_cid=c93d4ad9d7&mc_eid=7845af7088.

〔196〕*Id.*

〔197〕*See* J. Christopher Giancarlo（商品期货交易委员会代理主席）, LabCFTC: Engaging Innovators in Digital Financial Markets, Address to the New York FinTech Innovation Lab, May 17, 2017, http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-23.

〔198〕*See, e.g.,* Kyle E. Mitchell, *Seven Takeaways from the SEC DAO Report*, /DEV/LAWYER, https://writing.kemitchell.com/2017/07/25/DAO-Report-of-Investigation.html （“认为美国证券交易委员会”使用行业术语如用母语一般信手拈来）; Frances Coppola, Digital Coins And Tokens Are Just Another Kind Of Security, FORBES.COM（July 31, 2017, 8:17pm）, https://www.forbes.com/sites/francescoppola/2017/07/31/sec-tells-digital-coin-and-tokens-issuers-to-comply-with-securities-laws/#19faf7953bb1（认为在首次代币发行中，“是由程序员在负责操盘，而不是投资者，美国证券交易委员会已决定让他们承担责任，这无疑是正确的”）.

的法律制度的机制有很多。有些情况不需要法律介入,而在其他情况下,区块链仅起到补充作用,现有法律安排通常自动生效,无需与区块链相结合。然而,很多时候,必须采取积极措施来融合分布式分类账和中心化法律的精华。

(一)区块链和/或/作为法律

对于"代码即法",劳伦斯·莱斯格的观点是:无论是代码还是市场和规范都是一种监管形态。〔199〕其书名也对代码和"网络空间的其他法律"进行描述。至于两者孰优孰劣,还要以具体情况为准。举例而言,数字权利管理软件对内容使用的限制比著作权法更严格,因其忽略了诸如合理使用和首次销售原则之类的安全价值观。〔200〕因此,若存在 Lex Cryptographia,则关键问题就在于明确其相对于传统法律机制的优缺点。

法律制度和软件代码都能促进信任,也能摧毁信任。随着分布式分类账日益普及,其与法律需求此消彼长的片面观点越来越站不住脚。丝绸之路的骇客追缉令显示,区块链并不能完全规避法律实施,而 The DAO 攻击事件则反映出纯粹算法系统的治理局限性。但另一片面观点——监管者能够且应该像管理中心化系统一样管理算法系统——也是错误的。法律行为主体和开发新分布式平台的技术人员必须采取积极措施促进信任。如治理得当,区块链项目就能克服法律实施的局限性,反之亦然。

实现两种系统的结合有以下三种方法:区块链补充法律、区块链与法律互补以及区块链替代法律。

1.区块链补充法律

若现有信任结构普遍适用,依照现有的法律规则,区块链仍可作为额外的保障。在这种情况下,分布式分类账的主要价值就在于提升单一共享数据记录的速度和效率。〔201〕虽然区块链取代了各参与者之间极易出错的信息结构,但其无意颠覆整个产业结构。〔202〕

举例而言,美国对于房地产交易有完善的法律规则和交易实践。使用产权保险来保护购买者不受土地所有权瑕疵的影响。〔203〕正式规则和详实的规范相结合,创造了良好的信任环境。然而,由于产权保险多使用纸质记录,且必须在多方当事人之间流转,系统效率严重低下。高盛集团预测,从纸质记录转为分布式分类账能大幅提高效率、降低风险,每年能够为美国节省 20 至 40 亿美元的产权保险费用。〔204〕

在这种情况下,现有法律义务和中心化经营安排承担了维持交易信任的主要责任,区块链作为一种更优秀的记录机制参与其中。共享分类账数据的完整性十分可信。购买者与销售者及各中介机构(例如银行和经纪人)之间的信任关系保持不变。有关分布式分类账技术可行性的问题也与信任相关。〔205〕区块链的其他问题和局限性与信任的联系相对较弱,因为共享分类账无意取代追索权。

Corda(R3 金融行业协会项目)是另一例证。Corda 使用分布式分类账技术管理金融机构的协议,以此规避对账费用。〔206〕只有经认证的机构才能加入 Corda 网络。〔207〕尽管 Corda 利用共识型分布式分类账和智能合约,但其记录交易的数据结构并非区块链且不使用工作量证明。〔208〕

〔199〕*See* Lessig, *supra* note 22.

〔200〕*See id.*

〔201〕*See supra.*

〔202〕Cf. Building the Trust Engine, *supra* note 37, at 8("区块链可能会有效促使银行更好地完成工作,而非取而代之").

〔203〕产权保险仅在美国为必要。因为与世界上很多地方不同,美国有一个"按所有权登记"制度,而非"登记所有权"的制度。所有权转让的有效登记并不能确保一个不受剥夺的所有权。

〔204〕*See* Schneider et al, *supra* note 15, at 4–5.

〔205〕*See supra.*

〔206〕*See* Brown, Introducing Corda, *supra* note 52.

〔207〕*See id.*

〔208〕*See id.*

Corda 明确允许监管者介入。监管者可以操作“监督观测节点”,获取实时交易信息。〔209〕这一点很重要。事实上,区块链系统若能以促进监管监督为目的,而非像比特币协议一样排斥政府,必定能促进有效监管。共享分类账的实时透明能令监管者在事态恶化之前确认问题并及时应对。〔210〕其甚至能够直接在系统中建立合规机制。〔211〕

有分布式分类账从旁协助,建立信任可为万事俱备。区块链的作用仅限于保护共享分类账数据的完整性。如此使用区块链,真可谓大材小用。但对与监管者和其他政府行为主体而言,这种应用方式不会要求他们彻底改变其职能或工作原则,因而最容易被接受。这种方式低风险低回报。区块链作为现行法律制度的补充能够提高效率,降低交易成本,但很难转变产业结构或刺激突破性创新。

2.区块链与法律互补

第二种应用适用于法律系统信任崩溃或不足的情况。分布式分类账能够与之互补并扩展现有的信任结构。现在的问题是中心化安排规模有限,不能有效解决问题。区块链通常以与现有法律安排互补的方式推动新市场的发展。

以著作权法中的无主作品问题为例。〔212〕无主作品指的是权利人无法确定的作品。想要使用此类作品的人(例如想要将之作为影片资料的纪录片制片人)即便有心,也无法通过协商获取许可。因此无主作品就被法律边缘化。著作权侵权的法定赔偿风险很可能吓跑潜在的材料使用者,即使有些情况下相关资料本身就是公开的。著作权法设想的市场(其中作者能够控制并利用其作品赚钱)未能建立起来。无主作品为利用共享登记建立新市场提供了绝佳的机会。〔213〕所有人都能够获取区块链登记,且任何中介都不享有过多的网络权力。可以利用智能合约确保无主作品的使用者向(通过仲裁机制审核的)合法权利人支付许可使用费。此处的分布式分类账不会取代标准著作权法,反而帮助著作权法开拓难以涉足的领域。〔214〕

另一观点是令艺术家和其他内容创作者享有其作品权利的永久控制权。如今,数字版权管理系统由中介机构和分销商控制,而非创作者。因此,许多艺术家很难获得足够的补偿。包括 Ujo Music、PeerTracks 和 Open Music Initiative 在内的项目旨在利用分布式分类账分散数字权利的控制,还权于艺术家。〔215〕

这些风险项目同样面临固有权利机制的挑战。即使艺术家在技术上能够控制其作品产出,但在实际操作中,没有音乐市场的营销和分销,此举根本难以成行。考虑到所有的可能性,一小部分艺术家将灵活使用分布式权利平台,这也是现有仇视艺术家系统的一大进步。和互补性应用一样,以上区块链解决方案保留了习惯法(此处指著作权制度)。然而,这些解决方案对习惯法的应用并不符合现

〔209〕*See id.*

〔210〕*See* Building the Trust Engine, supra note 37, at 24(“在一个基于区块链的系统中,交易是及时的,分类账是公开的。监管机构可以随时查看系统内正在发生的事情”).

〔211〕*See id*. at 25.

〔212〕*See* Jerry Brito & Bridget Dooling, An Orphan Works Affirmative Defense to Copyright Infringement Actions, 12 MICH. TELECOMM. & TECH. L. REV. 75 (2005).

〔213〕*See* Patrick Murck, *Waste Content: Rebalancing Copyright Law to Enable Markets of Abundance*, 16 ALB. L.J. SCI. & TECH. 383, 416–17 (2006).

〔214〕同样,区块链也可以用来创建独特的数字资产,其可适用数字化作品著作权的长期首次销售原则。*See* Patrick Murck, *The True Value of Bitcoin*, CATO UNBOUND, July 31, 2013, http://www.cato- unbound.org/2013/07/31/patrick-murck/true-value-bit-coin.

〔215〕*See* Gideon Gottfried, *How “the Blockchain” Could Actually Change the Music Industry*, BILLBOARD(Aug.5,2015), http://www.billboard.com/articles/business/6655915/how-the-blockchain-could-actually- change-the-music-industry; Ian Allison, *Imogen Heap Shows How Smart Music Contracts Work Using Ethereum*, INT'L BUS. TIMES (Oct.4,2015,7:51 BST), http://www.ib-times.co.uk/imogen-heap-shows-how-music-smart-contracts-work-using- ethereum-1522331; Malcolm Gay, *Can Major Initiative Led by Berklee Solve Music -Rights Problems?*, BOSTON GLOBE, June13, 2016, https://www.bostonglobe.com/arts/music/2016/06/12/berklee-lead-musical-rights- initiative/aXBXC8adJgXE4IRRt8dcKO/story.html.

有信任结构的要求。因此,还需要对法律实施机构和分布式分类账的技术框架进行映射研究。

3.区块链取代法律

最后一类区块链法律应用并不支持传统法律实施。The DAO 事件证明了这一路径的危险。〔216〕然而,若法律实施不力,在特定情况下,区块链能够取而代之。若无可适用的法律规则,区块链规则或许能够有效填补空白。举例而言,发展中国家有数十亿人无法开立银行账户,且缺少获得便捷支付和低门槛信贷的机会。比特币和其他加密货币为解决这一问题提供一条捷径。〔217〕2017 年,联合国世界粮食计划署进行了一项成功的试验,使用以太坊区块链对约旦境内 10000 名叙利亚难民的食品援助发放情况进行追踪。〔218〕这一项目对传统法律实施难以为继时的责任承担作出了规定。

在世界许多地方,土地所有权记录并不完善且普通民众难以获取。秘鲁经济学家赫尔南多·德·索托(Hernando de Soto)指出,缺少健全的土地登记制度是阻碍发展中国家经济发展的主要原因。〔219〕世界很多地方开始利用区块链解决这一问题,包括加纳和格鲁吉亚。〔220〕

分类账之外的人类主体才是这些系统中的短板。某些腐败的地方土地管理局仍可拒绝在区块链准确记录信息,或无视上报的信息。由于当地合作伙伴不配合,由洪都拉斯初创公司公证通开展的区块链土地所有权记录项目还未实施就夭折。〔221〕因此,即使发展中国家对区块链的需求更大,此类项目也应转移到较为稳定的国家(例如格鲁吉亚)以及非常稳定的国家(例如瑞典)。

当然,若社群旨在规避法律责任,就会利用区块链替代法律。只有其目的是为了确保黑市(例如丝绸之路)盗亦有道时,区块链和法律实施才是完全对立的。以布宜诺斯艾利斯的优步为例,虽然该公司使用比特币来规避政府对支付的限制,但相关交易本身并不违法。〔222〕通过设置传统中心化支付方式之外的可信支付选项,加密货币赋予优步更多选择。〔223〕这种情况的确存在,但对分布式分类账而言并不重要。

(二)法律代码化

在前述三种情况中,区块链系统和法律制度的关系可谓时好时坏。区块链开发者不能无视法律,同时政府也不能无视区块链日益增长的重要性。想要缩小两者的差距,法律需相应改变。当监管者、立法者和法官直面基础性新技术带来的挑战和机遇时,法律改变就会水到渠成。采用明确的措施能加速法律代码化的进程。

1.安全港条款和沙盒

安全港条款是限制法律实施的正式监管规定。若公司能够采取足够的措施进行自我监管,安全

〔216〕*See supra* Text at Notes 126–130.

〔217〕*See* Mark S. Miller & Marc Stigler, THE DIGITAL PATH: SMART CONTRACTS AND THE THIRD WORLD, http://www.erights.org/talks/pisa/paper/index.html; Susan Athey, 5 Ways Digital Currencies Will Change the World, WORLD ECON. FORUM AGENDA BLOG (Jan. 22, 2015), https://agenda.weforum.org/2015/01/5–ways–digital–currencies–will–change–the–world/.

〔218〕*See* Leigh Cuen, UN Using Blockchain Technology to Help Refugees, Fight World Hunger, INT'L BUS. TIMES (May 4, 2017, 2:05pm), http://www.ibtimes.com/un–using– blockchain–technology–help–refugees–fight–world–hunger–2534759.

〔219〕*See* HERNANDO DE SOTO, THE MYSTERY OF CAPITAL: WHY CAPITALISM TRIUMPHS IN THE WEST AND FAILS EVERYWHERE ELSE (2000).

〔220〕*See* Laura Shin, *Republic of Georgia to Pilot Land Titling on Blockchain with Economist Hernando De Soto, BitFury*, Forbes (Apr. 21,2016,6:00pm),http://www.forbes.com/sites/laurashin/2016/04/21/republic–of–georgia–to–pilot–land–titling–on–blockchain–with–economist–hernando–de–soto–bitfury/#5a2979f36550; Roger Aitken, *Bitland's African Blockchain Initiative Putting Land on the Ledger*, Forbes, (Apr. 5, 2016, 2:44pm), http://www.forbes.com/sites/rogeraitken/2016/04/05/bitlands–african–blockchain–initiative–putting–land–on–the–ledger/#59ee9ab11029.

〔221〕*See* Pete Rizzo, *Blockchain Land Title Project 'Stalls' in Honduras*, COINDESK (Dec. 26, 2015, 15:31 UTC), https://www.coindesk.com/debate–factom–land–title–honduras/.

〔222〕*See supra* note 97.

〔223〕布宜诺斯艾利斯政府不能阻止乘客使用分布式比特币网络。然而,它可能针对瑞士 Xapo 公司发出指示,要求其提供可以在当地货币与比特币之间转换的借记卡。*See* Valenzuela, *supra* note 97.

港条款对其予以激励。这一条款同样对必要的特定行为进行规制。科技领域最著名的安全港条款就是 1996 年通过的《通讯法》第 230 条[作为《通信内容端正法》(CDA)的补充]。[224]该条规定,在线中介无需对流经其系统的内容负责。这一安全港条款是在商业互联网初期制定的,其适用范围并不确定。由于中介机构无义务采取积极行动,因而很难禁止明显有害的活动(例如网上骚扰行为)。[225]另外,CDA 安全港条款是在线中介机构快速发展的重要因素之一。[226]其对于用户主导的"网络 2.0"服务和社交媒体的普及尤为重要。[227]

以此为鉴,CoinCenter 针对区块链初创公司提出了一项新的安全港条款,[228] 促使立法机构宣布非担保服务提供商(对用户资金不享有控制权)不受资金转移主体相关规定的约束。由此可见,分布式分类账改变了资金转移主体和拥有资金的用户之间的关系。

比特币问世之前,拥有财富意味着可以任意处置。诸如 PayPal 之类的线上服务商有能力窃取用户存储在其上的资金或用于资助恐怖主义者。相比之下,在区块链中,许多行为主体(例如矿工、去中心化应用以及钱包软件提供者)能够接触交易记录,但若无管理用户账户的私钥,其便无能为力。只有经用户授权动用资金的担保交易所才能行使传统资金转移主体的职能。将所有权和控制权的区别引入法律安全港条款能够排除市场的不确定性,并增强法律制度和技术现实的契合度。

沙盒和安全港条款类似,但其受时间和规模限制。监管沙盒作为促进试验和创业活动的一种手段,能够令特定公司或活动不受监管。与安全港条款不同,沙盒并不一定是永久性的,通常只适用于新兴公司。互联网安全港条款的问题之一就是:其原本旨在帮助无力监管本平台内容的新兴公司,但最终获益的却是诸如谷歌和脸书之类的巨头。沙盒可用于发展初期的公司,并随其成熟而退出历史舞台。

英国主要的金融监管机构金融行为监管局(FCA)设立了金融科技沙盒项目,允许公司试用新服务。[229]申请进行沙盒试验的公司,若经批准,就会获得特别豁免和受监督的特别授权,可以无视监管问题开展试点项目。尽管 CFTC 的 LabCFTC 项目与上述项目方向一致,但这一时期美国并无可以与之相提并论的项目。[230]

相较于纽约比特币牌照使用的"不允即禁"方法,沙盒模式会鼓励"无许可创新",这种创新对互联网市场的发展相当重要。[231]软件开发者(包括建立区块链系统的开发者)的气质在互联网工程任务组(Internet Engineering Task Force)的座右铭(同时也是其决策的依据)中有所体现:"铁打的共识,流水的代码。"[232]精心设计的沙盒可以令初创公司上述代码的编写事半功倍,并令监管者能够清晰预见和理解可能产生的公共政策问题。

2.合约模块化

私法同样可以代码化。大多数商业合约本质上都是由律师组织并自定义的模块。有些部分对经

〔224〕47 U.S.C. 230.

〔225〕*See, e.g.*, Danielle Keats Citron and Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014).

〔226〕*See, e.g.*, Derek Khanna, *The Law that Gave Us the Modern Internet–and the Campaign to Kill It*, ATLANTIC (Sept.12,2013), https://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-internet-and-the-campaign-to-kill-it/279588/.

〔227〕*See id.*

〔228〕*See* Peter Van Valkenburgh, *Bitcoin Innovators Need Legal Safe Harbors*, COIN CENTER (Jan. 24, 2017), https://coincenter.org/entry/bitcoin-innovators-need-legal-safe- harbors.

〔229〕2016 年 7 月 11 日,在项目创新的两周年之际,金融行为监管局发布新闻稿,揭示了沙盒公司成功试验的信息。https://www.fca.org.uk/news/press-releases/financial-conduct-authority-unveils-successful-sandbox-firms-second-anniversary.

〔230〕*See* Giancarlo, *supra* note 197.

〔231〕*See* ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM (2016).

〔232〕*See* Andrew L. Russell, *"Rough Consensus and Running Code" and the Internet–OSI Standards War*, IEEE ANNALS OF THE HISTORY OF COMPUTING 28(3), at 48, 48 (2006).

营条款和特定情况下的应为之事进行阐述。在智能合约中,此类状况往往可以自动执行。[233]合约的其他部分就是非经营性或者法律条款,例如有关损害、赔偿、保密、法律适用和法院选择的规定。律师通常会重复使用格式条款,这些条款可以依照具体情况进行调整或协商。

为使上述合约起草程序更类似于智能合约的正式编码,合约条款可被视为使用标记语言的数字文件的组成部分。可从上述模块中提取模版,制定符合一般情况的基础协议。律师同样可以在自定义模版中发挥作用,决定使用何种变更以及协商有争议的条款。鉴于合约起草向法律工程学倾斜,对律师技能的要求也要作出相应改变。[234]为确保合约与当事人意图相符,可以采用法律审计(类似于软件开发公司广泛使用的安全审计)。[235]

许多项目正在开发此类系统。包括 Open Law(以太坊开发工作室 Consen Sys 开展的项目)、[236]初创公司和 Agrello、[237]R3 联盟的智能合约模版组[238]以及 CommonAccord 和 Legalese 的项目。[239]其中有些更侧重于非经营性条款,提升了法律合约起草程序的效率。其他项目则专注于可编入智能合约系统的经营性模版。通过预先标准化和审核智能合约的各元素,此类机制应可减少导致类似于 The DAO 黑客攻击的错误的发生。

未来代币简单协议(SAFT)是由律师事务所、天使投资集团 Angelist、Protocol Labs、IPFS 区块链分布式存储项目的母公司共同设计的标准协议。[240]这一协议旨在解决 ICO 法律地位的不确定性问题。SAFT 包括一系列用于组织未开始运营的区块链项目代币销售的文件,购买者向发行人支付加密货币作为出资,而发行人承诺会构建服务,并在项目投入运营之后立即对其签发代币。

SAFT 是一个私人项目,因此并不能解决 ICO 是不是证券的问题。但其解决了监管者十分关注的有关投资者保护的重大问题。[241]事实上,SAFT 令预运行项目代币销售的法律协议更加类似于相关智能合约对该系统拟签发代币的授权方式。Protocol Labs 开展的 Filecoin 代币销售是 SAFT 的初次实践,募集到 2.5 亿美元,是迄今为止规模最大的 ICO。[242]

传统法律要求对区块链系统仍具重要性,这是启动合约标记语言和 SAFT 之类的项目的前提。举

〔233〕Christopher D. Clack, et al, Smart Contract Templates: Foundations, Design Landscape and Research Directions, ARXIV PREPRINT arXiv:1608.00771 (2016), https://arxiv.org/pdf/1608.00771.pdf. (将操作方面定义为,"我们希望实现自动执行的合同部分,这些部分通常是考虑到各方将采取的明确行动且因此与合同履行有关").

〔234〕关于律师技能,这或许能为合法的黑客创造一种新的合适的职业。在 DAO 攻击之后,安全专家 Robert Graham 建议说,"过去,人们雇佣律师来审查复杂的合同。在将来,他们将需要雇佣黑客。合同签订之后,我倾向于雇佣一个非常厉害的黑客来审查代码,以便于发现一些威胁我利益的非法入侵。"Robert Graham, Ethereum/TheDAO attack Simplified, Errata Security (June 18, 2016), http://blog.erratasec.com/2016/06/etheriumdao-hack- similfied.html#. V2wGDOYrKV5.

〔235〕现在已经有技术审计公司审查智能合约代码的漏洞或安全漏洞。See Alyssa Hertig, Blockchain Veterans Unveil Secure Smart Contracts Framework, COINDESK (Sept. 15, 2016, 18:14 UTC), https://www.coindesk.com/blockchain-veterans-unveil-secure-smart-contracts-framework/.传统的审计公司也在考虑如何参与这个新的世界。正如普华永道会计师事务所区块链策略师 Grainne McNamara 在金融服务会议上所说的,"我们正在研究如何利用该技术来审计这项技术。"American Banker Blockchains + Digital Currencies Conference (June 13, 2017) (作者转录), http://conference.americanbanker.com/conferences/blockchains/.

〔236〕*See* Introducing OpenLaw, Consensys (July 25, 2017), https://media.consensys.net/introducing-openlaw-7a2ea410138b.

〔237〕Clause.ioSets Out Strategy with its Smart Contract Engine, ARTIFICIAL LAWYER (July 6, 2017), https://www.artificiallawyer.com/2017/07/06/ clause-io-sets-out-strategy-with-its- smart-contract-engine/; Agrello Becomes 1st LegalTech Co. To Launch Its Own Digital Currency, ARTIFICIAL LAWYER (July 17,2017), https://www.artificiallawyer.com/2017/07/17/agrello-becomes-1st-legaltech-co-to-launch- its- own-digital-currency/.

〔238〕*See* Clack, et al, supra note 233.

〔239〕http://commonaccord.ord; http://legalese.com.

〔240〕http://commonaccord.ord; http://legalese.com.

〔241〕SAFT 本身只是一个发行代币的承诺。因此,它不能保证这些代币本身不是受监管的证券。

〔242〕*See* Stan Higgins, *$200 Million In 60 Minutes: Filecoin ICO Rockets to Record Amid Tech Issues*, COINDESK (Aug.10, 2017, 21:43 UTC), https://www.coindesk.com/200-million- 60-minutes-filecoin-ico-rockets-record-amid-tech-issues/.

例而言，SAFT 依照美国证监会的 D 条例或众筹条例（证券发行登记要求的例外之二）组织代币发行。与之相伴的还有诸多限制。依照 D 条例开展的发行（例如 Filecoin 的 ICO）只能以合格投资者（经验证资产净值超过 100 万美元或单人收入超过 20 万美元、家庭收入超过 30 万美元的投资者）为发行对象。而依照众筹条例展开的发行只能募集 100 万美元出头的资金。尽管存在认证障碍，Filecoin 仍成功吸引了巨额资金，证明这些并非难以克服的困难，但偏离了 ICO 作为不受监管的全球性募资工具这一概念。

随着区块链相关机制日益标准化和模块化，法律实施和代码执行之间的界限必将愈发模糊。这在衍生品交易中已初露端倪：国际掉期与衍生品协会（ISDA）规定的标准化主协议和术语可以在不使用分布式分类账的情况下实现广泛的交易自动化。〔243〕

（三）代码法律化

正如监管者和律师能够适应区块链环境，分布式分类账系统也能逐渐适应法律实施。想要实现这一目标，有以下三种主要途径：促进法律条款和智能合约条款的融合；促进传统法律实施机制和智能合约的融合；促进类似法律的治理程序和区块链平台的融合。

1.合约融合

提升区块链系统与法律实施的契合度最简单的方法就是将两者合二为一。即使依照合同法的基本原则，法庭可以强制执行智能合约，其作用也与合约的基本救济机制不同。〔244〕智能合约能够在事前有效地罗列出预期条件和结果，并确保满足条件后对应结果的产生。法律合约能够在意外事件必然发生的情况下，有效作出梳理和补救。但两者无法共存纯属无稽之谈。智能合约与法律合约各自为政才是问题产生的根源，The DAO 倒闭就是典型例证。

另一方法就是将智能合约和法律合约配对。2004 年，在加密货币出现之前，信息安全专家伊恩·格里格（Ian Grigg）首次提出了这一观点，将之作为李嘉图金融票据数字交易平台的一部分。〔245〕根据李嘉图（Ricardo）之定义，合约包含三个组成部分：法律条款（合约的可读文本）、计算机代码（智能合约的可执行步骤）和参数（影响计算机代码执行方式的变量）。法律条款包含计算机代码的密码哈希字符串，确保法律代码与相关智能合约的一一对应关系。同样的，智能合约文本也包括法律合约的密码哈希字符串。因此，两者必然存在联系。若智能合约出现问题，可以通过法律合约解决该问题。由于这一合约配对结构是为李嘉图系统创立的，因此格里格将之命名为李嘉图式合约。〔246〕

类似于萨博最初的智能合约概念，李嘉图式合约的理论构造产生于区块链之前。〔247〕自以太坊成功实施区块链智能合约，这一结构得以重见天日。英国巴克莱银行领导的 R3 联盟的子群、〔248〕Monax Burrow 软件（如今是超级账本开源项目的一部分）〔249〕以及 OpenLaw〔250〕等项目都利用智能合约和法律合约的共同哈希探索相应解决方案。

通过这一方法，人工合约和智能合约通过数字签名相互参考。The DAO 的服务条款规定，算法合

〔243〕ISDA White Paper, The Future of Derivatives Processing and Market Infrastructure. (Sept. 2016), https://www2.isda.org/attachment/ODcwMA==/Infrastructure%20white%20paper.pdf.

〔244〕*See* Werbach and Cornell, *supra* note 25.

〔245〕*See* Ian Grigg, The Ricardian Contract, Proceedings of the First IEEE Workshop on Electronic Contracting (2004).

〔246〕*See id.*

〔247〕伊恩·格里格当时正在构建的李嘉图平台从未面世。

〔248〕*See* Clack et al, supra note 233; Bailey Reutzel, *BNP Paribas Works with Blockchain Startup to Open Source Law*, CoinDesk (May 5,2016,16:28 BST), http://www.coindesk.com/commonaccord-legal-smart-contracts-prove-beneficial-one-bank- veritcal/; Ian Allison, *Barclays' Smart Contract Templates Stars in First Ever Public Demo of R3's Corda Platform*, Int'l. Bus. Times (Apr.18,2016, 15:45BST), http://www.ibtimes.co.uk/barclays-smart-contract-templates-heralds-first-ever-public-demo-r3s-corda-platform-1555329.

〔249〕*Putting the Contracts in Smart Contracts*, Eris: Legal, https://erisindustries.com/components/erislegal/.

〔250〕*See supra* note 236.

约无需进行可读解释,与之相比,本方法中人工合约和智能合约是相互依存的关系。法院或其他决策者可以依照常规合约理解智能合约的意图,而智能合约负责处理合约的执行。〔251〕

每一智能合约并不一定附有自定义的人为协商合约。就当下的合约系统而言,企业–消费者协议和低价值协议的格式条款将广泛普及开来。很多情况下,争议解决的费用会超过"简单粗暴"依赖机器自动操作可能得到的赔偿。对中介机构进行监管(比如登记)可以排除为相关智能合约指定法律条款的必要性。随着区块链系统日益普及,将客户、普通法以及示范立法相结合解决常见问题是大势所趋。

2.预言机和计算法院

合约融合将法律协议与智能合约的实质性条款相结合。另一种不同的方法是将某些执行元素从智能合约自动化系统中剔除。换言之,智能合约能够自动生效,但无法完全自动执行,以此规避自动化代码主导型执行的模糊性和局限性。

许多智能合约必定要与外界接触。举例而言,在区块链中,以特定价格购买证券的买入期权可以在算法上执行,并以比特币或其他加密货币进行支付。但区块链并不了解股票价格。必须通过连接外部的自动化数据源或人类仲裁者获取该信息,再提供给智能合约。这种外部信息源被称为预言机。〔252〕有些预言机就是带有智能合约接口的传统数据源,允许智能合约自动处理相关数据。世界最大的商业出版公司之一汤森路透集团着力于开放其数据源,使其与智能合约预言机功能一致。〔253〕Oraclize 是一家专注于数据源—预言机转化的初创公司。〔254〕

莱特和德·菲利比指出,法院或私人行为主体可将预言机扩展至争议解决领域。〔255〕预言机可以是人。以简单智能合约为例,合约双方均拥有密钥,第三把密钥由专家仲裁员持有。合约至少需要有两把密钥方可生效。若合约各方认同合约已被充分履行,则会提供各自的密钥,智能合约生效。若存在争议,则由仲裁员居中仲裁。仲裁员要么提供其密钥,与要求执行合约的当事方一同执行该合约,要么拒绝提供,阻止交易达成。这一模式照搬了法律仲裁程序。

智能合约可在默认情况下吸收仲裁机制或重算规定。可以被设定为只在极端情况下生效,并通过多重签名程序设置高垒。这对解决诸如 The DAO 黑客攻击之类的极端事件大有裨益。还可以利用智能合约创造私人争议解决的常规途径,即像企业–消费者格式合同一样采用争议仲裁。著名区块链投资者和初创公司 21 的创始人巴拉吉·斯利尼瓦桑(Balaji Srinavasan)指出:"随着时间流逝,区块链将提供'服务型法治',以此对特拉华州衡平法院进行国际化和程序化补充。"〔256〕

区块链的分布式性质可能要求引入新的分布式执行机制。〔257〕举例而言,尽管世界知识产权组织

〔251〕在 DAO 攻击之后,研究人员提出了一种相当于撤销智能合同的技术机制,此举不一定涉及司法人员。See, e.g., Ittay Eyal and Emin Gun Sirer, *A Decentralized Escape Hatch for DAOs*, HACKING, DISTRIBUTED (July 11, 2016, 2:42pm), hackingdistributed.com/2016/07/11/decentralized– escape–hatches–for–smart–contracts/(提出了一种"逃脱舱口"机制,该机制一旦启动,所有的交易都将被缓冲并通过众包途径进行恢复)。Bill Marino and Ari Juels, Setting Standards for Altering and Undoing Smart Contracts, Int'l Symposium on Rules & Rule Markup Languages for the Semantic Web (Springer 2016)(详细说明修改或撤销智能合约的方案).

〔252〕*See Smart Oracles: A Simple, Powerful Approach to Smart Contracts* (July 17, 2014), https://github.com/codius/codius/wiki–i/Smart–Oracles:–A–Simple,–Powerful–Approach–to– Smart–Contracts.

〔253〕Maria Terekhova, Thomson Reuters is Makign a Blockchain Push, Business Insider (June 15, 2017, 10:42am), http://www.businessinsider.com/thomson–reuters–is–making–a– blockchain–push–2017–6.

〔254〕http://oraclize.it.

〔255〕*See* Wright and De Filippi, *supra* note 23, at 50.

〔256〕*See* Balaji S. Srinivasan, Thoughts on Tokens, NEWS. 21.CO.(May 27,2017).

〔257〕以太坊创始人 Vitalik Buterin 构思一种"分散的法院"制度,以解决纠纷。See Vitalik Buterin, Decentralized Court, Reddit /r/etherium, https://www.reddit.com/r/ethereum/comments/4gigyd/decentralized_court/ (last visited July 6, 2016); Izabella Kaminska, Decentralised Courts and Blockchains, FT Alphaville (Apr. 29, 2016), http://ftalphaville.ft.com/2016/04/29/2160502/decentralised–courts–and–blockchains/.

已经制定了统一域名争议解决规则(UDRP)来处理网络域名的商标争议,但为了迎合区块链争议的需求,可能需要建立新的国际仲裁网络。[258]由于仲裁决定在某些情况下可以直接在区块链执行,且可能以点对点的方式进行适用,区块链仲裁系统仍有别于其他现有的仲裁系统。[259]2016 年,安德里亚斯·安东诺普洛斯(Andreas Antonopoulos)和帕梅拉·摩根(Pamela Morgan)提出了去中心化仲裁和调解网(DAMN)。[260]

计算法院,或称计算陪审团,是一种更为投机的方法,有些区块链项目正对这一方法进行开发。这些机制通过预测市场对群众智慧加以利用,取代仲裁员解决争议的方式。[261]Augur 以太坊预测市场也在探索这一方法。现金预测市场(例如 Intrade)被监管者叫停的原因之一是其可能涉及非法或不道德使用。例如,谋杀岳母 / 婆婆的预测市场可能会造成大麻烦。

Augur 提议通过预测结果验证报告程序解决不道德市场的问题。在 Augur 系统中,市场参与者购买被称为信誉币的代币。[262]当有人创建一项合约,例如预测总统会在某一特定时间内遭到弹劾,用户以信誉币缴纳保证金。若其预测准确,则能赢得更多信誉币;若预测失败,就会失去交纳的保证金。系统会随机选取一些报告人(职能类似于陪审团),负责验证预测结果。这些报告员也要交纳保证金。用户可以对报告提出质疑,若第二次随机选取的陪审团认可该质疑,则提供错误信息的报告人会失去其保证金。这一程序的复杂性毋庸置疑,且的确有理由怀疑其可行性。但这一程序为按照法律体系的既有体制运行去中心化区块链科技提供了可行方法。

诸如此类的自愿机制都可能被纳入区块链应用,在某些情况下,甚至具有法律上的强制执行性。可利用所有的激励和治理机制来鼓励对理想方式的探索。此外,依照《联邦仲裁法》,在不存在诈骗的情况下,法院应当接受私人仲裁决定,以此类推,立法也应赋予经合理设计的区块链争议解决系统相同的法律效力。[263]

3.链上治理

区块链网络的最大弊病之一就是其治理机制的基本规则难以改变。若系统拥有完善的机制,能够对共识规则或其他技术属性进行考量和调整,则这类系统本质上就不是去中心化的。其与行业标准主体或开源项目类似,通过集体协议而非公司管理层的分层法令改变规则。

相较于通用电气,以太坊与维基百科更为类似。维基百科是新的组织方法与广泛用户参与相结合改变市场的典型例证。[264]维基百科不仅仅取代了其他百科全书,更创造了史上最大的开放信息源。若以太坊也能取得如此成就,势必会创造传奇。且以太坊和其他区块链网络的潜力更大。由于具有充分的变革性,这些系统需要利用去中心化方法来改变其治理机制。

尽管比特币没有正式的治理结构,其开发者设置了名为 BIP 9 的自愿信号机制。[265]依照 BIP9,矿

〔258〕*See* Luke A. Walker, *ICANN's Uniform Domain Name Dispute Resolution Policy*, 15 BERKELEY TECH L. J. 289 (2000).

〔259〕*See* Abramowicz, *supra* note 41, at 405.

〔260〕*See* Michael del Castillo, *Lawyers Be DAMNed: Andreas Antonopoulos Takes Aim at Arbitration With DAO Proposal*, CoinDesk (May 26, 2016, 23:57 BST), http://www.coindesk.com/damned-dao-andreas-antonopoulos-third-key/. 它以纽约公约为基础,根据该公约,65 个国家同意其法院执行公认的仲裁员的决定。仲裁制度的权衡是将中介机构重新引入去中心化的区块链环境中。See James Grimmelmann and Arvind Narayanan, The Blockchain Gang, SLATE.COM FUTURE TENSE (Feb. 16, 2017, 10:05am),http://www.slate.com/articles/technology/future_tense/2016/02/bitcoin_s_blockchain_technology_won_t_change_everything.html.("仲裁员既能将车还给你,也能将它收走,他是区块链应该消除的那类中间人").

〔261〕*See* Rizzo, supra note 164.

〔262〕Tony Sakich, Jeremy Gardner & Joey Krug, What is Reputation?, http://augur.strikingly.com/blog/what-is-reputation.

〔263〕Federal Arbitration Act, 9 U.S.C. § § 1-16 (2012).

〔264〕*See* YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006); DON TAPSCOTT & ANTHONY D. WILLIAMS. WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING (2008).

〔265〕BIP 表示比特币改进提案。这是一种机制,根据因特网工程任务组的"征求建议书"进程,可以对比特币提出技术修改,供社区审查。

工可以在系统中公告,其有意且准备对系统进行变更。这一程序被用来进行 Seg Wit 升级。当系统提示计算机哈希能力已达 80%,Seg Wit 会在区块链网络自动激活。〔266〕BIP 9 为有争议的比特币协议升级设置了原始的投票机制,同时也对链上治理提出了更多展望。升级的批准并无统一的标准,主要由提议升级的人决定。更重要的是,BIP 9 只负责发出信号,并不负责执行政策。有关比特币扩容的争论仍需要获得广大网络参与者的一致认可。

目前有关主体正努力创建真正的链上治理。名为 Rootstock 的项目尝试在比特币区块链上建立智能合约侧链,依照这一内置程序,矿工和用户均有权对网络变更进行有约束力的投票。Decred 和 Tezos 则致力于建立带有治理机制的全新区块链。这些系统使用不同的算法,令网络参与者有权对协议变更投票,变更经投票通过的,会自动生效。2017 年春,Decred 利用治理机制成功执行了投票代币分配算法的变更。〔267〕Tezos 在规模最大的首次代币发行中募集到超过 2.3 亿美元,并从其治理方法中攫取了巨大利益。〔268〕

这些系统均有局限性。其对分布式分类账系统规则的诸多方面进行内化处理。但这些系统利用民主投票的硬编码规则实施变更。这或许是一种优秀的治理方式,甚至像温斯顿·丘吉尔所说的那样,是"多害相权取其轻",其并不完美。总会有人对不完美的治理结构进行改进。此外,人类需要对网络参与者投票的规则变更下定义,若该变更被通过,还需编写软件予以实施。链上治理系统令区块链的运行向人性化法律或治理体制靠近,但若想真正融合区块链和法律,传统法律制度必须作出相应改变。

结　论

分布式分类账是这 20 年来首项基础技术,其潜在影响可媲美互联网。随着对中心化权力结构的信任逐渐减弱,区块链的"不信之信"提供了一个更具优势的选择。经济的进一步增长是技术进步、采用模式、分布式分类账平台的商业创新和区块链信任结构治理问题的解决共同作用的产物。人们普遍认为,法律和监管是上述程序的主要障碍,但这一观点是错误的。虽然法律过严会扼杀区块链或者将之逼入地下,但过松同样会造成上述后果。

区块链仍处于初生阶段。距中本聪发布比特币白皮书还不到十年,以太坊也是在 2015 年才正式启动。区块链市场在不断壮大,路径依赖问题也并不严重,未来可能出现的风险现在担心还为时尚早。现在应当以法律和代码的融合作为主要任务。监管者、立法者和法院可采取措施,为实验创造明确的空间。区块链开发者同样需要发掘两者的共同之处。

和互联网一样,区块链也是一项足以影响世界的基础技术。〔269〕此外,法律与分布式分类账相互依存,共生共荣。

〔266〕这个过程在技术上被称为 BIP 91。

〔267〕*See* Christine Chiang, *Decred Launches Decentralized Voting Process for Blockchain Protocol Changes*, BRAVENEWCOIN (June 17, 2017), https://bravenewcoin.com/news/decred- launches-decentralized-voting-process-for-blockchain-protocol-changes/.

〔268〕*See* Alice Lloyd George, Behind the Scenes with Tezos, a New Blockchain Upstart, TECHCRUNCH (July 12, 2017), https://techcrunch.com/2017/07/12/behind-the-scenes-with- tezos-a-new-blockchain-upstart/.

〔269〕*See* Iansiti & Lakhani, *supra* note 16 (描述基础技术).