区块链与未来法治

郑　戈*

内容摘要：区块链（blockchain）是一种基于互联网的全新的分布式基础架构与计算范式，利用有序的链式数据结构存储数据，利用共识算法更新数据，利用密码学技术保障数据安全。它的第一个应用领域是比特币，但其应用前景却不限于加密货币。区块链也不完全等同于分布式账本，它可以是任何分布式的数据库。在国家治理和社会治理领域，技术与法律具有相互替代性，如果在某一社会场景中技术解决方案的成本低于法律解决方案，技术工具便可能取代法律形式成为秩序生成的主要手段。区块链技术所促生的分布式可验证数据库和智能合同便具有这种改变技术与法律边界、形成新的治理模式的潜质。但技术解决方案在提升效率和确定性的同时也可能威胁到法律的非效率价值，比如平等和公正。如何在吸纳技术所带来的制度创新的同时避免进入技术决定一切的社会物理学世界，保存法律的价值向度，这是本文试图回答的问题。

关键词：区块链　比特币　分布式账本　智能合同　未来法治

一、引　　论

区块链是一种结合对等网络（P2P）技术和加密技术而创造出不可更改的分布式可验证公共数据库的数字技术。如果这个账本记录的是货币，区块链就是加密货币，比如比特币、莱特币、以太币等现有的数百种数字货币。但这个账本可以被用来记录任何数据结构，包括所有权证明、身份和认证信息、合同等。区块链是一种熊彼特意义上的制度技术，在一定程度上可以替代某些法律形式。在这个意义上，区块链技术被称为“分布式账本技术”或“无需信任的共识引擎”。〔1〕账本之所以重要，是因为它是市场经济的基础性制度。马克斯·韦伯认为理性化的记账技术是资本主义的核心技术，而这种技术在双重簿记中得到最明显的体现。〔2〕从账本中衍生出来的问责制是现代公法体系中的基础性概念

*上海交通大学凯原法学院教授、博士生导师，上海高校特聘教授（东方学者）。

基金项目：上海高校特聘教授（东方学者）岗位计划资助。

〔1〕Swanson, T. （2014） Great Chain of Numbers. Creative Commons, available at www.ofnumbers.com/the-guide/ （accessed 30 April 2017）.

〔2〕Max Weber: *Economy and Society: An Outline of Interpretive Sociology*, Guenther Roth & Claus Wittich ed., University of California Press, 1978 （second printing）. V.I, p.91—92.

之一：任何公职承担者都应当严格区分公共账目和自己的私人账目，防止混淆和利益冲突，确保公共权力的行使服务于公共利益。[3]正因如此，一种无需中介机构和监管机构来加以验证的、不可篡改的、分布式的账本技术显然具有带动制度创新的意义。

在2018年年初召开的达沃斯世界经济论坛上，区块链再次成为与会的政商领袖和学者们重点讨论的议题之一。包括施蒂格利茨[4]和罗伯特·希勒[5]等诺贝尔经济学奖得主在内的众多人士都提出了一个类似的观点：比特币和作为比特币之技术基础的区块链有着不同的未来发展前景，尽管比特币可能前途未卜，但区块链技术却还远未发挥它的巨大潜质，具有无可限量的前景。在达沃斯会场之外，越来越多的政治、法律学者开始意识到区块链作为制度技术或法律技术的属性，从而超越了经济学者将其视为金融技术的狭小视野，[6] 并开始讨论这种技术普遍应用到法律领域后可能带来的范式转换。

实际上，将比特币与支撑其应用的区块链技术区分开来一直是主流的声音。多数评论者认为，哪怕比特币最终退出历史舞台，区块链技术也会继续发挥其革命性的力量。《经济学人》2015年的一篇文章将区块链称为“信任机器”。“区块链使得彼此之间并无信任感的人们得以无需借助一个中立的中央权威而进行合作。简单地说，它是一部创造信任的机器。”[7]在同年的一篇文章里，杜克大学法学院的一位学生也明确指出要区分作为一种技术应用的比特币和作为比特币之基础技术的区块链，并且指出区块链的广阔应用前景不会因比特币的兴衰而受到根本的影响。[8]“因为区块链是一种认证和核实技术，它可以促成更有效率的权利转移和产权认证。因为它是编程化的，因此可以按照事先设定的条件来执行‘智能’合同。因为它是去中心化的，因此可以在最低限度信任和无需依赖集权式机构的情况下发挥这些功能。因为它是无边界、无摩擦的，因此能够为价值单位的交易提供一种更便宜、更快捷的基础设施。”[9]

我国对待区块链和比特币的态度也体现了这种主流共识。一方面，针对比特币等加密货币高风险的特质，中国人民银行等五个部门于2013年12月3日联合发布了《关于防范比特币风险的通知》，明确表示比特币“不是真正意义的货币”，并要求现阶段各金融机构和支付机构不得开展与比特币相关的业务。2014年3月，中国人民银行又向各分支机构下发了《关于进一步加强比特币风险防范工作的通知》，禁止国内银行和第三方支付机构为比特币交易平台提供开户等服务。[10]另一方面，政府高度重视区块链作为新一轮信息技术革命中的核心技术之一的意义，在国务院《“十三五”国家信息化规划》（2016年12月）等文件中强调要发展区块链技术；工信部于2016年10月发布了《中国区块链技术和应用发展白皮书》，为行业提供了发展方向指引；2017年5月16日，国内首个区块链标准《中国区块链参考架构》正式发布，确定了区块链核心功能组件的范围和标准。同时，我国还作为16个全权成员国之一积极参与了国际标准组织（ISO）的区块链技术标准委员会（ISO／TC307）的标准起草工作，与其他成员国一起塑造着全球区块链技术标准的未来。

区块链技术首先是一种基于互联网的、去中介化的转移货币、资产和信息的技术。[11]交易在一个

〔3〕郑戈：《公民权的身份、财产与契约维度：一种基于公共信托原理的公民权理论》，《交大法学》2012年第1期。

〔4〕“Stiglitz at Davos,” http://wn.com/Joseph_Stiglitz_At_Davos_2018.

〔5〕“Robert Shiller Says Bitcoin is an ‘Interesting Experiment’,” https://www.cnbc.com/2018/01/26/robert-shiller-says-bitcoin-is-an-interesting-experiment.html. Robert J. Shiller, “What Is Bitcoin Really Worth? Don’t Even Ask,” *New York Times*, December 15, 2017.

〔6〕对于区块链作为制度技术或法律技术的属性及其应用方案，最系统的论述，参见Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Harvard University Press, 2018。

〔7〕“The Trust Machine,” Economist, October 31, 2015, https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.

〔8〕〔9〕Trevor I. Kiviat, “Beyond Bitcoin: Issues in Regulating Blockchain Transactions,” 65 *Duke Law Journal* 569 (2015).

〔10〕参见上海新金融研究院课题组：《数字货币与金融技术监管的崛起》，《新金融评论》2017年第6期。

〔11〕Swan, 2015, ix.

只能添加新数据(区块)而不可修改的数据库中按时间顺序被验证、执行和记录,并被盖上“时间戳”,由此形成的全部数据全天候地向公众开放,随时供查阅和验证。正如简单邮件传送协议(SMTP)构成电子邮件系统的基础协议,使得使用不同网络服务商提供的邮箱的用户得以顺畅地传输邮件并在不同终端应用软件里打开和阅读这些邮件一样,区块链协议使得用户可以快捷地传送货币和其他数据库,不管他们的银行帐户或终端是什么。如果说传送信息的互联网是第一代简单网络的话,区块链则是传送价值的智能网络。[12]由于区块链技术是互联网基础上的一种创新架构,甚至被称为“新一代互联网”,它必然会像互联网一样改变法律所要调整的社会关系,同时也会改变法律本身的运作方式。

笔者正是在区块链技术在加密货币之外的领域(包括法律领域)得到越来越广泛应用的背景下介入相关讨论的一次尝试。全文分为五个部分,第一部分是引论;第二部分讨论区块链技术所欲解决的现实问题;第三部分介绍区块链技术作为一种“法律技术”对现有法律秩序的冲击;第四部分讨论主权国家主导的法律制度对区块链技术的规制和驯服;第五部分分析区块链技术在辅助和强化现有法律秩序方面的应用前景。

二、无需信任的共识机制:区块链技术所针对的问题

人工智能和区块链都是在互联网基础架构的基础上产生的技术创新,但两者的算法设计和功能却是截然相反的。

首先,它们在数据处理方面贯彻不同的设计理念。人工智能旨在利用已经进化到物联网阶段的互联网所生成的海量数据来训练神经网络等能够进行“机器学习”的算法,从而使机器在视觉(图像识别)、语言(自然语言处理)和推理、预测方面能够完成人类需要运用智能才能完成的任务。基于这种设计理念,人工智能无节制地利用着数据,以至于有人说:“授计算机以数据,够它用一毫秒;授计算机以搜索,够它用一辈子”。虽然某些具体人工智能产品的开发需要以人工筛选和标注数据作为前期准备工作,但总体上说人工智能技术的发展取决于数据的开放性、互联互通性和大量级属性。而区块链则是在点对点(P2P)技术的基础上通过公钥/私钥加密算法来实现数据的准确传输的技术,它体现的核心价值是私密性、准确性和可验证性。

其次,上述设计理念决定了它们的不同功能:人工智能主要被用来处理人力已无法处理的海量数据,从中找出人类行为的规律和模式,对未来作出预测,并根据这种预测量身定制地影响个人的消费选择和其他决策,使用的方法包括有针对性地投放广告(百度、淘宝、京东等平台企业常用的方法)、定制新闻(今日头条等内容服务商常用的方法)以及利用消费者弱点获取额外利润(比如大数据杀熟或抢票加速器,携程等预定平台常用的方法)。而区块链则不具有如此“狡猾”的特点,它的功能不是去学习、预测和影响人类行为,而是防止人类篡改已被确认的数据,如实记录已经完成的交易和其他行为,并在此基础上自动执行行为的后果。从这个意义上讲,区块链更像是法律执行器:当条件A、B、C满足时,准确地记录下这些条件发生的时间和状态,盖上时间戳,然后让结果R发生。法律是社会学家莫顿所称的“自我实现的预言”:[13]如果立法界定某些情形为真实的,那么它们就其结果而言就是真实的,法律系统会借助国家强制力来令法律后果发生。而区块链技术一方面可以验证导致某种后果发生的事先设定的条件是否已经发生;另一方面可以以此为前提自动让这种结果发生,比如在网上交易中自动执行“智能合同”。

从知识脉络上看,人工智能和区块链分别是维纳的控制论和香农的信息理论的当代体现。香农

〔12〕Melanie Swan and Primavera de Filippi, “Introduction to Toward a Philosophy of Blockchain: A Symposium,” *Metaphilosophy*, Vol.48, No.5, October 2017, pp.603—619, at 605

〔13〕R. K. Merton, ‘The Self-Fulfilling Prophecy’ (1948) 8 The Antioch Review 2, 193.

的信息理论追求信息传播的速度、保密性和完整性。他认为信息量多寡可以用不确定性和惊讶程度来衡量，如果完全确定（套路），则没有信息；如果存在随机概率，则有信息。随机概率（或最大不确定性）被称为熵，这个从热力学中借用来的概念是指稳定的无序状态。由于香农所关注的是在给定信息传递渠道约束条件下如何以最短的时间传递最大量的信息，所以他主张在信息中移出任何冗余的符号（比如去掉所有元音字母），只要这样不影响信息接收端复原内容。〔14〕这种概率论和极简主义的设计思路也体现在区块链技术中。而维纳则试图利用信息来控制环境，因此更侧重信息的完整性和可操纵性，体现的是决定论模式。人工智能通过对大数据的分析来预测社会行为中的隐藏模式，从而实现对人类行为的控制，这恰和维纳的思路吻合。〔15〕

第三，从上述两点来看，人工智能主要是一种生产技术，用于创造价值；而区块链则主要是一种交换技术，用于交换价值。人工智能可以被用来在给定目标的前提下寻找最优解决方案，实现利润最大化或治理效率最大化，而区块链则主要被用来记录已创造出来的价值的真实状态，确认权利归属，并执行交易决策。套用一句广告词的说法，区块链不生产价值，它只是价值的搬运工。但整个现代市场经济和相关的法律制度都是在解决资源／价值的有效配置和流通问题，因此区块链具有冲击整个市场经济法律秩序的潜在能力。

信任，无论是传统社会中基于家族纽带和熟人关系而形成的人际信任，还是非个人化的法律所确保的、由各种中介机构所提供的制度化信任，是市场经济的基石。1788年6月20日，在弗吉尼亚州批准《美利坚合众国宪法》的会议上，制宪元勋麦迪逊说道："信任的流通比货币的流通更好。"〔16〕法律一直在设计和执行各种信任机制，以拓展人类活动的疆域、增进社会总体福祉并维持稳定的社会秩序。在中世纪的欧洲，随着海上贸易的发展，投资者与航海贸易商之间形成了受法律保障的分成合伙制，以确保有冒险精神的商人能够获得投资者的资金，而投资者也能够在无法有效监督资金使用过程的情况下得到恰当的回报。〔17〕这里体现的是以法院作为中介的信任关系。此种关系中的各方在彼此之间不用形成基于家族纽带、伦理或感情的信任，而只需要信任有能力执行法律的司法机构就可以了。这是资本主义产生的制度基础。进入现代社会，由中立的监管机关和司法系统来裁判和执行的法律关系更成为陌生人社会有效运转的基础。可以说，法治就是一种信任机制，是父权主义的传统治理方式和以"熟人社会"为特征的共同体瓦解后维持社会秩序和可预期人际关系的依赖国家主导的各种中介机构来运行的信任机制。

但中介机构在这一过程中积聚起了巨大的权力。本来应当不偏不倚地验证事实、解决纠纷、执行合同和规则的中介机构越来越多地借助手中的权力来为本机构及其人员谋取利益。谋取利益的方式有"俘获"和"寻租"两种形态。所谓"俘获"，是指监管机关的利益与监管对象的利益耦合，被监管对象"俘获"，罔顾公共利益地为监管对象服务，并因此不再值得公众信任。普通消费者之所以对俘获现象没有反制能力，是因为"消费者是最缺乏组织性并且在一般情况下最无效力的利益群体。尤其是对于长期的消费者利益来说，基本上完全没有为其代言的游说者"。〔18〕而"寻租"则是指中介机构通过创设不必要的验证、审批和监管程序来增加自身的权力和福利（包括闲暇，比如上班时看报、聊天甚至打麻将），创造谋取利益的机会，从而损害经济效率和社会正义，增加法律运作的成本。〔19〕

〔14〕C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, July and October, 1948, Vol.27, 379—423, 623—656.

〔15〕N. Wiener, Cybernetics: Or Control and Communication in the Animal and the Machine (Cambridge, Mass: MIT Press, 1948) and idem, The Human Use of Human Beings: Cybernetics And Society (Boston: Da Capo Press, 1988).

〔16〕"Statement of James Madison at the Virginia Convention (June 20, 1788)," in 4 *The Debates in the Several State Conventions on the Adoption of the Federal Constitution* 538, Jonathan Elliot ed., 2d ed. 1836.

〔17〕Max Weber: Economy and Society: An Outline of Interpretive Sociology, Guenther Roth & Claus Wittich ed., University of California Press, 1978 (second printing). V.I, p.95.

〔18〕Richard A. Posner, *Natural Monopoly and Its Regulation*, Cato Institute, 1999, p.67.

〔19〕Anne O. Krueger, "The Political Economy of the Rent-Seeking Society", American Economic Review, LXIV (3), June 1974, 291—303.

英国历史学家帕金森通过对各种官僚机构进行历史研究发现：对于任何一个官僚机构（这里指行使公共权力的任何“中介”机构），无论分配给一项工作的时间有多长，这项工作总是会在最后期限来临时才告完成，他把这个规律称为“帕金森定律”。不过，“帕金森定律”这一名称后来也被人们扩展适用于这本书中提出的其他一些关于行政机构的一般性命题，这些命题主要包括：（1）行政领导均喜好增加部属——不论机关的实际工作量有多少，其人员总会稳步增加。（2）机关成立的时间越长，其成员的素质就越低——因为行政领导喜欢选用才智不如自己的人，以免制造职位上的竞争者。（3）机关开会时间的长短，与议题的重要性成反比——因为小事无关痛痒，且大家都略知一二，所以发言踊跃。然遇大事则大家或因不懂、或因害怕承担责任而噤若寒蝉，不愿发言，所以会议早早结束。（4）机关乐于采用“委员会”形式的管理方式，以协调内部利益。但委员会日趋涨大，人浮于事，便产生组成核心决策小组的需要。核心小组又日趋涨大。（5）机关内部的行政工作效率日趋低落，而其办公场所和设施的豪华程度则日趋上升，两者竟成反比。（6）机关凡有可用之经费必会尽快用完，不然会导致下一年度的预算惨遭削减。[20]“徒法不足以自行”，法律依靠各种“中介”机构来操作，但这些中介机构都难以避免会陷入“帕金森定律”的怪圈，损害人们对法律本身的信任。

除此以外，官僚化的中介机构有着极高的运作成本和规避风险的倾向，因此它们往往设置极高的确权门槛，将大量的穷人和中小企业排除在正式的信用体系之外，使他们无法获得贷款和其他融资支持，无法将死的财产变成活的资本，因此无法享受资本收益。这些被正式金融资本体系排斥在外的人占全球人口的绝大多数，经济学家德·索托估计这个数字达50亿人。[21]

因此，用技术来取代中介机构作为“信任机器”是人类社会的一种持久追求。互联网的出现给这种追求提供了新的发展平台。早在互联网出现之初，就出现了一群后来被命名为“密码朋克”（cypherpunk）的无政府主义者，试图用公钥－私钥加密技术来实现个人之间的匿名交流。依靠无法追踪的网络和“防篡改的、执行加密协议的盒子”，人们可以无需借助任何中介、也无需借助任何受监管的市场来做生意、谈判达成电子合同。在这种情况下，不仅人际信任不再必要，每个人都无需知道对方的身份，只要信任代码就可以了。[22]区块链技术就是在密码朋克的传统里出现的一种技术。

2008年11月1日，在爆发于华尔街并蔓延到全球的金融危机以小布什签署总额达7000亿美元的政府救市方案而告一段落之后不到一个月的时候，一位化名中本聪的“密码朋克”在metzdowd.com网站的密码学邮件列表中发表了一篇题为《比特币：一种点对点式的电子现金系统》[23]的文章，宣布了一种新技术的诞生。这种技术可以被用来打造一个电子支付系统，“它基于密码学原理而不基于信用，使得任何达成一致的双方，能够直接进行支付从而不需要第三方中介的参与”。为了达到这一目的，中本聪综合了此前便已经存在的若干技术，而搭建了一种全新的架构，这个架构包括交易和验证两个环节。在交易环节采取公钥－私钥加密技术，公钥私钥成对出现，由随机算法生成私钥，由椭圆曲线算法从私钥生成公钥，这种算法可以确保从公钥无法反推出私钥，公钥可以公布，相当于银行收款账户，而私钥则用于数字签名，类似于收款人签名，以确认交易完成。为了确保交易的唯一性，防止一物二卖或双重支付，交易信息必须公开宣布，供整个系统的所有参与者验证。而验证环节则包含这样一些技术方案：（1）时间戳服务器：对以区块链形式存在的一组数据实施随机散列而加上时间戳，并将该随机散列进行广播。每一个随后的时间戳都对之前的一个时间戳进行增强，这样就形成了一个链条。时间戳可以

〔20〕C. N. Parkinson, Parkinson's Law, and Other Studies in Administration, Houghton Mifflin Co, 1957.

〔21〕参见［秘鲁］赫尔南多·德·索托：《资本的秘密》，于海生译，陕西师范大学出版社2009年版；［秘鲁］赫尔南多·德·索托：《另一条道路》，于海生译，华夏出版社2007年版。

〔22〕Timothy May, “The Crypto Anarchist Manifesto,” 1988, https://www.activism.net/cypherpunk/crypto-anarchy.html.

〔23〕Satoshi Nakamoto: “Bitcoin: A Peer-to-Peer Electronic Cash System,” http://bitcoin.org/en/bitcoin-paper. 中译本参见：http://www.8btc.com/wiki/bitcoin-a-peer-to-peer-electronic-cash-system。

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确权、公证、智能合同等时间敏感的场景奠定了基础。因此，区块链技术的鼓吹者们常说：区块链阻止我们就历史说谎。[24]加盖了时间戳的已完成交易数据会形成一个区块。(2)共识机制：就是区块链节点(系统中的每一台计算机或"矿机"都是一个节点)就区块信息达成全网一致共识的机制，用以确保最新区块被准确添加到区块链、节点存储的区块链信息一致不分叉以及抵御恶意攻击。中本聪本人提出的共识机制是工作量证明，它的本质是算力决定权力，付出最大计算工作量的节点取得创造下一个区块的权力，为此节点消耗自身算力尝试不同的随机数，进行指定的哈希计算，并不断重复该过程直到找到正确的随机数，完成此任务后，才能生成区块信息，经其他节点验证后链接至区块链。其他的共识机制还包括权益证明、权益证明+工作量证明、瑞波共识协议等，其目的都是为了确定节点的"投票"权重。(3)激励机制：为了鼓励节点参与验证工作，使新的交易能够不断被新的区块所记录，中本聪提出将每个区块的第一笔交易作特殊化处理，产生一枚由该区块的创造者拥有的电子货币。在加上"交易费"(一笔输出值小于输入值的交易所产生的差额)收益，便足以产生足够的激励让众多的节点参与验证过程。由于这种机制所产生的新币类似于矿工挖出的金子，所以参与者(节点)被称为"矿工"，区块创造过程被称为"挖矿"，用于"挖矿"的计算机被称为"矿机"。

整个区块链网络的运行包含生成过程有这样几个步骤：(1)新的交易向全网进行广播；(2)每一个节点都将收到的交易信息纳入一个区块中；(3) 每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明；(4)当一个节点找到了一个工作量证明，它就向全网进行广播；(5)当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性；(6)其他节点表示他们接受该区块，而表示接受的方法，则是在跟随该区块的末尾，制造新的区块以延长该链条，而将被接受区块的随机散列值视为先于新区块的随机散列值。

中本聪的这一套技术方案回应了金融危机中银行、券商等中介机构失信以及监管失灵所导致的用技术取代信任的需求。耶鲁法学院教授乔纳森·梅西在2008年金融危机后出版的一部著作中指出，金融危机的教训表明，旨在补救信用匮乏问题的会计师事务所和律师事务所等中介机构自身也面临信用危机，而美国证监会这样的替代信用的监管机构则陷入自身的官僚逻辑，它的使命变成了维护自身的利益，包括提高自己的预算和权力，以及为那些位高权重者谋求晋升之机。他指出："在这场金融危机期间，信用评级机构似乎被发行方所操控。然而，美国证监会被大型信用评级机构操控得似乎更加彻底。"[25]既然信用评级机构本身没有信用，监管机构又被它"俘获"，人们便需要寻找在低信任度环境下交易的技术化替代方案："由于金融交易存在重大利益，在低信任度及低声誉环境里的人们就有着强烈的动因来开发技术性的替代品，从而让人们在像投资银行这类缺乏可信声誉的机构环境里参与金融交易。与这一假设相一致，在金融领域，一些特别重要的制度最好是被解释成方便人们在低信任度环境下进行交易的机制。"[26]完全无需信任、无需中介机构的区块链技术显然正适合用来解决梅西教授所指出的这一类普遍问题。而且，由于交易和验证全过程的匿名性，区块链技术可以实现对个人隐私的最大化保护，不像中介机构那样为了验证而索取很多的个人信息。

三、作为"法律技术"的区块链

法律和技术都是解决人类社会基本问题的手段，两者在许多领域可以相互替代。2017年诺贝尔经济学奖得主理查德·泰勒和法学家卡斯·桑斯坦在《助推》一书里就介绍了很多利用人们的认知规

〔24〕Nigel Dodd, "The Social Life of Bitcoin," *Theory, Culture, and Society*, 2017.

〔25〕[美]乔纳森·梅西：《声誉至死：重构华尔街的金融信用体系》，汤光华译，中国人民大学出版社2015年版，第181页。

〔26〕同上书，第211页。