律来进行技术设计，从而无需借助法律强制而诱导出有益社会的行为方式的例子。〔27〕而法学家莱西格在网络法经典名著《代码》中则多次强调“代码就是法律”，它控制着人们的网上行为。〔28〕随着移动智能终端的普及和互联网的升级，线上、线下生活的界限已经越来越模糊，赛博空间已经成为现实空间的一部分。因此，代码不仅控制着人的网上行为，它控制着人的行为。作为一种由代码构成的、在互联网上运作的创新性架构，区块链也被越来越多的人认为是一种“法律技术”，即可以替代法律功能的技术，甚至可以作为经济学家威廉姆森所说的“资本主义经济制度”中的一种。〔29〕就目前已有的应用状况来看，它的确在这样几个方面冲击着现有的法律秩序。

首先是在货币、金融领域，区块链技术已促生了数百种加密货币，其中排名前十的加密货币市场总值已达到4500多亿美元，而且其价格大起大落，冲击着全球金融市场及其法律监管机制。谈到货币，很多人可能会把它想象为一种交易工具、一种媒介、一种等价流通物。但货币具有根本的宪法意义。发行货币和维持货币信用都是主权国家或类国家政治体的主要权力。现代主权概念的提出者让·博丹曾经说过：“至于铸币的权力，其性质与立法权相同，只有享有立法权者才有权规制货币。”〔30〕第二次世界大战以后形成的布雷顿森林体系通过将美元与黄金挂钩、其他国家货币与美元挂钩、实行可调整的固定汇率等措施使美元成为最主要的国际储备货币，缔造了美元这种主权货币统治世界的时代。但这个体系在1971年随着德国和荷兰实行浮动汇率、美国于同年8月15日宣布实行“新经济政策”停止外国央行用美元兑换黄金之后瓦解。〔31〕在这个国际货币体系形成的过程中，各主权国家并没有丧失对本国货币的控制权。

就在宣告自己的技术方案之后两个月，即2009年1月，中本聪发布了开源的第一版比特币客户端，宣告了比特币的诞生。他同时通过“挖矿”获得了50枚比特币，产生第一批比特币的区块被称为“创始区块”。随着比特币数量的不断增多（虽然中本聪为比特币的总量设定了一个限制，最终产生的比特币数量，准确的说是20999999.97690000个，比2100万少一点。在达到这个总量之前，新增的比特币数量每四年减少一半）以及其他加密货币的不断涌现，以国家信用为基础的法定货币以及国家控制货币以及通过货币政策来对经济进行调控的能力必然受到影响。比如，欧洲央行在2015年的一份报告中指出，由于比特币的价格非常不稳定，而且接受比特币作为支付手段的商家数量还非常有限，所以比特币目前还不能作为价值载体或交换手段，因此不能被称为货币。但是，随着比特币和类似的虚拟货币的稳定化，它们有朝一日会成为货币。〔32〕一种不经过任何银行和其他中介机构的跨境自由流转的货币会给监管带来很多问题，给洗钱、贩毒、暗网交易创造更大的空间，损害主权国家以征税为主要手段的财政汲取能力。

实际上，比特币等加密货币背后的意识形态基础正是对国家极度不信任的自由至上主义。这种意识形态的主要代表是哈耶克，他在1977年的一篇文章中写道：“不只是货币给我们惹来的麻烦，还有资本主义经济的不稳定性以及政府的扩张，都完全是因为政府拒绝授权自由企业来提供其所需要的好的货币，如果不是政府禁止的话，这种好货币早就在竞争中脱颖而出了……我毫不怀疑竞争在提供市场妥善运行所需的货币制度方面更具创造性。”哈耶克认为通行的货币理论中存在两个误解，一是必须有一种法定货币；二是格雷善定律（Grasham’s Law，劣币驱逐良币），所以必须有政府监

〔27〕〔美〕理查德·H·泰勒、卡斯·R·桑斯坦：《助推》，刘宁译，中信出版社2009年版。

〔28〕Lawrence Lessig, Code: Version 2.0, New York: Basic Books, 2006, Chap.1.

〔29〕Sinclair Davidson, Primavera De Filippi, and Jason Potts, “Blockchains and the Institutions of Capitalism,” Journal of Institutional Economics, 2018(1), pp.1—20, p.16.

〔30〕Jean Bodin, *On Sovereignty*, edited by Julian H. Frankin, Cambridge University Press, 1992, p.78.

〔31〕Benn Steil, *The Battle of Bretton Woods: John Maynard Keynes, Harry Dexter White, and the Making of a New World Order*, Princeton University Press, 2013.

〔32〕European Central Bank, Virtual Currency Schemes–A Further Analysis15 (2015), https://www.ecb.europa.eu/pub/pdf/other/virtual–currencyschemesen.pdf.

管。〔33〕虽然哈耶克没有活到比特币出现的那一天，但他显然会欢迎这样一种完全摆脱了包括政府在内的各种中介机构和监管机构的货币。〔34〕而哈耶克的观点在思想史传统上来看也并不新奇，它只是约翰·博奇协会创办者罗伯特·韦尔奇观点的另一种表述。韦尔奇认为主权国家的货币政策是经济问题的症结所在，通货膨胀是隐形征税。直到今天，仍有不少自由至上主义者主张废除中央银行。比如，《美联储传》的作者指出，终结美联储有七大理由：1.它无法达成它所宣称的目标；2.它是侵犯公众利益的卡特尔；3.它站在高利贷体系的最顶端；4.正是它催生了对我们最不公平的税收；5.它鼓励战争；6.它让经济处于不稳定状态；7.它是极权主义的工具。〔35〕有学者指出这种“右翼极端主义”思想正是写入了比特币代码系统的政治诉求。〔36〕

伦敦经济学院的多德教授指出：“作为货币的比特币要想取得成功，只有靠作为意识形态的比特币的失败。这种货币依靠的是它所体现的意识形态试图否定的东西，即货币对社会关系和信任的依赖。比特币之所以能够作为货币而取得成功，恰恰是因为围绕着它而成长起来的共同体。”〔37〕这段话深刻地揭示出了比特币的困境：它的鼓吹者宣称可以完全去中介化、去权威化、去人格化，但他们恰恰是通过形成一个圈子并劝说更多的人进入这个圈子才使比特币能够被越来越多的人接受作为支付手段。同时，它的成功还是因为以它为支付手段的交易量与以法定货币作为支付手段的交易量相比是微不足道的。而它的去中介化潜质只有当交易量达到一定规模的时候才可能发挥出来，但在那个临界点到达之前，它的增长就会破坏现有的金融秩序，引起主权国家的干预或完全禁止。

其次是智能合同，即一种由计算机代码表述并自动执行的合同，其履行由区块链架构加以保障。换句话说，智能合同是一串计算机代码，其中包含一套具体的指令，指明当特定的条件得到满足时，一项交易便会完成。1997年，时任乔治·华盛顿大学法学院教授的尼克·沙波发表了一篇题为“智能合同”的文章，其中写道：“智能合同不涉及人工智能。它是一套用数码形式明确表达的承诺，其中包含当事人根据这些承诺作出履行的约定。”〔38〕沙波认为智能合同的经典现实例子就是自动售卖机，你投进钱币，它吐出商品和找零，无需任何中介。其他例子还包括销售终端机（POS）、电子数据交换机（EDI）、环球同业银行金融电讯协会结算系统（SWIFT）、自动清算系统（ACH）以及联邦储备通信系统（FedWire）。合同设计需要达到四个目标：（1）可观察性，涉及会计；（2）可证明性，涉及审计；（3）默契性，无需第三方介入；（4）可执行性，与此同时减少执行的成本。这四个目标之间有冲突，比如可观察性和可证明性与默契性往往不可得兼，但加密技术可以帮助我们设计出兼顾四个目标的智能合同。

在这篇文章里，沙波第一次提出了加密区块这个概念。〔39〕加密技术的目的是增加合同表述的含混性而不损害其内容和执行精确性。他指出：“与通常所认为的透明带来安全的观点不同，含混对于安全而言往往十分重要。加密协议是围绕被称为密钥的混淆点而建立起来的。一个密钥的无边无际的未知随机性使得系统的其他部分可以是简单和公开的。一个大位数的随机数字的含混性是如此巨大，以至于碰运气的猜测不可能蒙对，而破解它需要耗尽整个宇宙的时间，这就是加密协议以及随后的智能合同建立于其上的基础。”沙波虽然在这篇文章里提出了打造智能的合同的理论，但并没有提出具体可行的技术方案。中本聪所开发出的区块链技术可以整合分散的计算资源（即分布式的虚拟机）来制造含混性，并在包容含混性的状态下验证和执行合同，图灵完整的编程语言使交易主体可以

〔33〕Friedrich A. Hayek, “Toward Free Market Money,” Wall Street Journal, August 19, 1977.

〔34〕Henrik Karlstrøm, “Do libertarians dream of electric coins? The material embeddednessof Bitcoin,” Scandinavian Journal of Social Theory, 2014, Vol. 15, No. 1, 23—36.

〔35〕[美]G.爱德华·格里芬：《美联储传：一部现代金融史》，罗伟等译，中信出版集团2017年版，第576页。

〔36〕David Golumbia, *The Politics of Bitcoin: Software as Right-wing Extremism*, Minneapolis: University of Minnesota Press, 2016, 15

〔37〕Nigel Dodd, “The Social Life of Bitcoin,” *Theory, Culture, and Society*, 2017 Online First Edition, p.3.

〔38〕N. Szabo, “Smart Contracts: Formalizing and Securing Relationships on Public Networks,” First Monday 1997, 2 (9), http://journals.uic.edu/ojs/index.php/fm/article/view/548.

〔39〕因此有人猜测他就是“中本聪”。

自行起草和部署智能合同。如今，智能合同已经在多个区块链系统中得到应用。

第三个应用领域是数字财产权。“物权法是关于登记册和账本的法律。物权法保护下的财富大多记录于账册系统中，它告诉人们谁拥有什么。”〔40〕但现有的物权登记系统却不能适应信息化时代的需求，关于物权归属、物权变动、物权负担、物权价值、物权损益的信息散见于不同行政部门和法院的档案和案卷之中，难以查询，无法整合，并且往往没有实时更新。物权法亟待一场信息技术革命，而作为分布式公共账本技术的区块链是解决上述问题的有力工具。

同时，信息时代的经济形态已经发生了很大变化，很大一部分社会财富创造者是每一个上网并贡献数据的人。但法律并没有发生相应的变化，以解决社会化生产的价值分配问题。因此，所谓分享经济实际上变成了聚合经济，平台企业依靠众人的劳动积聚起巨额财富，而没有相应的机制来回报生产者。这些生产者同时也是消费者，他们是在消费过程中贡献了数据，所以也没有寻求回报的意识。网络价值生产有三个层次：首先是价值的生产；其次是价值的记录；第三是价值的实现。价值的生产日益无形化，它取决于某种特定的社会需求是否得到满足。价值的记录涉及系统化的协调评估。而价值的实现需要由类似于比特币那样的根据工作量或贡献来给予回报的机制。基于区块链技术的反馈机制。区块链技术提供了一套完整的解决方案，可以作为使共享经济真正具有共享性的技术手段。凯文·凯利写道：“区块链的一个重要方面还在于它是一种民众公有。没有一个人真正拥有它，因为每个人都拥有它。作为一个变得数字化的发明，它也在倾向于变得共享；在它变得共享的同时，它也变得无主化。当每一个人都‘拥有’它时，也就没有人拥有它。实际上，这就是我们通常所指的公有财产或民众公有。”〔41〕

无形资产在国民经济中所占的比重不断增加是一个持续的过程，这种变化没有体现到企业的财务报表和国家的各种经济数据统计中。因为用于培育无形资产的开支没有被计算为投资，而是被视为日常开支。无形资产投资具有更强的规模效应和更大的积淀成本，能产生更大的溢出效应和同步效应，因此更倾向于导致社会两极分化。创造无形财富的人在这个过程中很难获益，因为无形资产往往无法被记帐、被确权。〔42〕区块链技术也有助于解决这个问题。法律代码化的早期尝试是数字权利管理（DRM），它将著作权法条文转化成自动执行的代码，限定着作品可被复制的次数、防止修改并自动收取使用费。〔43〕区块链技术可以更进一步，完成包括确权、有偿使用收费和转让在内的全流程自动化处理。

加密数字货币只是区块链的第一个应用领域，从技术上来看，区块链更近似于作为互联网基础协议的传输控制和网络互联协议（TCP／IP），而不是一种应用程序。如果说TCP／IP为信息互联提供了基础，区块链则为价值互联提供了通道，两者都是属于互联网的“基础设施”。以上所列举的只是区块链作为法律技术的三个应用例子。实际上，在所有涉及记录和验证的领域，包括司法过程中的证据保存、提交和验证，都可以借助区块链技术来完成。

四、法律对区块链技术的驯服和利用

正如互联网本身一样，区块链也经历了从突破现有法律框架、冲破现有制度约束到被法律驯服和利用的过程。当然，这是一个正在进行、远未终结的过程。在互联网发展的早期，其鼓吹者认为

〔40〕Joshua A. T. Fairfield, “BitProperty,” 88 *Southern California Law Review* 805 (2015), p.807.

〔41〕［美］凯文·凯利：《必然》，周峰等译，电子工业出版社2016版，第136页。

〔42〕Jonathan Haskel and Stian Westlake, Capitalism Without Capital: The Rise of the Intangible Economy, Princeton University Press, 2018, pp.240—241.

〔43〕Bill Rosenblatt, William Trippe and Stephen Mooney, 2002. Digital rights management: Business and technology. New York : M&T Books.

它可以将个人从主权国家的支配中解放出来，实现真正的自由。克林顿在一次演讲中称：要规制互联网就像“想把果冻钉在墙上一样”，[44]是一种徒劳的企图。但时至今日，人们已经承认，国家不仅可以规制互联网，还可以借助互联网实现对社会的全面监控，使奥威尔在《一九八四》中描写的场景成为现实。这并不是国家单方面努力的结果，而是公民“自愿配合”的结果。正如所有的技术一样，互联网技术本身是中立的，既可以成为自由技术，也可以成为控制技术。自由需要追求自由的人付出艰辛的努力，就互联网时代的自由而言，人们需要驾驭Zittrain所说的那种创生性的机器，这种计算机采用开源性操作系统和软件开发平台，个人电脑有什么功能，完全取决于每个人的自主设计，就像无线电爱好者自己组装的通讯设备一样。而整个互联网也必须是一个开源的创生性网络，[45]每个人分散的创造性活动汇聚成社会生产，[46]再通过共享机制实现“各尽所能，按需分配”。但实际的情况是，大多数人不愿意付出努力去学会控制自己的电脑，而是更愿意使用一切都设计好的、所见即所得的操作界面，哪怕在此过程中丧失自己的自由和隐私。这促成了像苹果计算机和IPhone这样的“智能终端”的兴起。所谓智能终端，实际上是机器变得智能，而人变得愚蠢。“对于像Iphone这样的设备而言，一切都服从于显示。”[47]IPhone使得用户不用去考虑它的运行原理，不用去四处搜索和下载软件，不用关注显示之外的任何事情，而只用轻松地享受显示屏所带来的各种便利和乐趣。这显然给智能终端制造商和政府监视、追踪和操控用户提供了极大的便利。

同样，区块链技术要实现它的“解放”潜质，也需要其使用者付出艰辛的努力。而实际上除了少数有理想有抱负的加密朋克和“技术呆子”以外，大量的参与者是不愿意动脑筋而只想挖到更多比特币的人。区块链设计者和鼓吹者所使用的一些术语，比如计算能力、解答复杂的数学问题、工作量证明等，使得“挖矿”工作显得很有技术含量。而实际上所有的计算都是计算机完成的，矿工只需要开机点开程序就可以了。整个“挖矿”工作是一个耗费大量电力和计算机算能的毫无创造性的过程。用一位学者的话来说：“在这种由内而外的社会资本提取术的微观经济学中，我们所有人都是魔法世界的金矿矿工，将自己垃圾化以度过每一天。”[48]在这种情况下，区块链上的“工作”仍然受制于线下的生产关系、社会分配格局和法律。有钱的投资者可以购买大量的“矿机”，雇用许多“矿工”，为自己挖取比特币。而黑客可以黑进别人的计算机系统，盗用别人的计算能力来为自己挖矿。与此相比，人类中介服务虽然也成本巨大，但却孕育了律师、公证、银行等高端职业，除了提供就业机会外还满足了人的自我实现需求。区块链拓展人类自由和促进社会平等的潜质还远远没有发挥出来。卡尔·波兰尼在《大转型》中指出：实现“自我调整的市场”这种“彻头彻尾的乌托邦”的唯一办法是通过一个强有力的干预型国家的支持。他机智地把这种系统称为“计划的自由放任式资本主义”：“自由放任这种东西一点儿都不自然，自由市场从来不会仅仅通过让事情自然发展就自动形成？自由放任政策本身是由国家强力推行的。”[49]同样，区块链最终会成为自由技术还是控制技术，也取决于国家如何通过法律和政策来调整它的发展方向。

区块链本身存在的一些问题给国家通过法律称干预提供了切入口。首先，区块链技术所支撑的加密货币由于匿名性和无中介性成为洗钱、贩毒、贩卖人口以及贩卖军火等暗网交易（或称深网交易）的热门支付手段。2015年5月29日，暗网黑市“丝绸之路”的网站站长罗斯·乌尔布里奇被判处不可保释的终身监禁，该网从事贩毒和洗钱，便是以比特币为支付手段。美国《银行业保密法》（BSA）规定

〔44〕“Remarks by President Bill Clinton on China,” Paul H. Nitze School of Advanced International Studies, Washington, DC, March 8, 2000, http://www.usembassy-china.org.cn/press/release/2000/clinton38.html.

〔45〕Jonathan Zittrain, *The Future of the Internet and How to Stop*, Yale University Press, 2008, Chap.1.

〔46〕关于社会生产的分析，参见：Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Market and Freedom*, Yale University Press, 2006。

〔47〕Brian Merchant, *The One Device: The Secret History of the IPhone*, Little, Brown and Company, 2017, p.331.

〔48〕Benjamin H. Bratton, The Stack: One Software and Sovereignty, MIT Press, 2015, p.127.

〔49〕Karl Polanyi, The Great Transformation, Boston: Beacon Press, 1957, p.218, 250, 145.

银行和其他金融机构必须满足各种登记和记录保存要求，所有提供货币服务的企业都必须在财政部注册并且建立自己的反洗钱和客户身份识别机制。2013年3月，美国财政部金融犯罪执法网络（FinCEN）将这些规则扩展适用到用“可兑换的虚拟货币”进行的交易的参与者，主要是交换者和管理者，不包括用虚拟货币购买产品和服务的消费者。此外，美国商品期货交易委员会（CFTC）也把比特币等加密货币界定为《商品期货交易法》所规定的“商品”，因此认为自己有权规制加密货币基础上产生的衍生金融产品，包括掉期合约。纽约州金融服务部于2015年6月3日发布了旨在规制“虚拟货币行业”的BitLicense规范框架，要求通过第三方传递虚拟货币、为他人代持虚拟货币、经营买卖虚拟货币的业务、经营兑换虚拟货币的业务以及控制、管理和发行虚拟货币都必须事先获得许可并接受监管。〔50〕与此类似，日本也于2016年通过法律第六十二号修正了《资金结算法》，其中第三章第二节专门针对虚拟货币，规定只有经由首相注册登记后方可从事虚拟货币交易。2017年3月24日公布了《关于虚拟货币交换业者的内阁府令》，作为上述规定的实施细则。这些法律规制手段都抓住了虚拟货币与现实世界的接口作为切入点来进行规制：直接接受虚拟货币作为支付手段的商家毕竟还不多，虚拟货币要实现其“货币”价值，还是需要兑换为各种法定货币，而这个过程会受到严格的监管。

其次，区块链技术所保障的匿名性其实仅仅是指参与者可以使用化名，但流出和流进某一地址的所有交易都会记录在区块链中，很容易追踪和分析出交易者的身份。“在计算机科学中，匿名指的是具备无关联性的化名。所谓无关联性，就是指站在攻击者的角度，无法将用户与系统之间的任意两次交互进行关联。在比特币中，由于用户反复使用公钥哈希值作为交易标识，交易之间显然能建立关联。因此比特币并不具备匿名性。”〔51〕这说明技术和人类操作的法律一样都不是完美的，可能需要相互配合、相互补充才能实现更好的权益保护。这种可追踪、可定位、可识别的化名系统一方面使恶意的私人攻击者有机可乘，另一方面也为政府监控区块链上的交易活动提供了通道。

第三，借用区块链技术所支撑的数字货币概念，欧洲央行和我国政府都正在考虑发行法定数字货币，这种货币一方面会吸收借鉴先进成熟的数字技术，尤其是区块链；另一方面把传统货币长期演进过程中的合理内涵和法律保障机制继承下来，因此具有很强的竞争力。最主要的是，因为它本身就是“法定”的，所以不存在比特币等加密货币所面临的法律风险。在未来的法定数字货币与私人基于区块链技术而开发出来的数字货币的竞争中，后者将因其规避国际法和国内法规制的特性而受到主权国家和国际组织的抵制。2017年12月，西方各大媒体都刊文报道了朝鲜在制造和利用比特币方面的举国努力。

结　语

诺贝尔经济学奖得主罗伯特·希勒对人类法律和监管机制充满信心，认为其中体现着人类追求共同福祉的价值选择。“我们应该把很多对未来的畅想都寄托于代表金融体系的各类制度的发展上。当今信息技术的发展令我们感到炫目，而这些发展应该能够以简洁的方式与金融创新相互作用。但归根到底，金融制度的发展比硬件和软件的发展更重要。金融系统实质是一个信息处理系统——一个建立在人力基础而非电子元件基础之上的系统，而且人工智能离彻底取代人类智慧还有很远的路要走。”〔52〕笔者基本赞同这种观点，认为人类法律和各种为法律正常运作而存在的中介机构并不能完全被技术取代。不过，技术可以被用来弥补现有法律运作方式中的不足，尤其是取代其中不必要的、为官僚机构增加自身权力和寻租而设置的验证和审批程序，从而提高法律运作的效率，提升其公正

〔50〕参见Trevor I. Kiviat, “Beyond Bitcoin: Issues in Regulating BlockchainTransactions,” 65 Duke Law Journal 569 (2015).

〔51〕张宪、蒋钰钊、闰莺：《区块链隐私技术综述》，《信息安全研究》2017年第11期。

〔52〕[美]罗伯特·希勒：《金融与好的社会》，束宇译，中信出版社2012年版，第349页。

品质。

马克思有针对性地强调:“工人要学会把机器和机器的‘资本主义应用’区别开来”,〔53〕“同机器的资本主义应用不可分离的矛盾和对抗是不存在的,因为这些矛盾和对抗不是从‘机器本身’产生的,而是从机器的‘资本主义应用’产生的”。在本文的语境中,这些警示的意义在于让我们看到比特币等加密货币与支撑它们的基础性技术区块链有着根本的区别。正如几位学者所言:“我们主张区块链是这里的真正创新,无论加密数字货币最终被证明有或者没有价值,它们都只是这种技术的第一次应用尝试。”〔54〕

笔者的主要观点是:(1)区块链技术是大数据所催生的“社会物理学”的一部分,它旨在用数理方法处理社会关系,因而可能取代法律的一部分作用。从根本上说,区块链是一种法律技术或制度技术,将会直接改变法律(包括各种规制手段)的形态;(2)正如早期的互联网一样,区块链技术体现着自由至上主义的政治意识形态,试图通过去中介化的技术手段来削弱(如果不是瓦解)政府和金融机构存在的必要性。但同样像互联网一样,它最终会变成政府控制社会和市场的新工具;(3)技术只可能改变法律运作的方式,减少法律运作的成本,但不可能完全取代法律。

〔53〕[德]马克思、恩格斯:《马克思恩格斯文集》(第五卷),人民出版社2009年版,第493页,第508页。

〔54〕Sinclair Davidson, Primavera De Filippi, and Jason Potts, “Blockchains and the Institutions of Capitalism,” *Journal of Institutional Economics*, 2018(1), 1—20, p.2.