·全国青年理论创新奖征文选登·

法律与技术如何相处：区块链时代犯罪治理模式的双重重构

赵小勇

【内容摘要】区块链时代犯罪治理面临的危机，主要体现为区块链技术的“去中心化”消解了责任主体概念，“匿名性”阻塞了传统归责路径，代码自动执行排斥外部力量对犯罪过程的介入及“分布式”特征削弱了网络空间中的主权管辖等方面。我国近年对 P2P 网贷和网约车的治理历程，揭示了实现法律与技术之间的和谐相处之道——不能依靠管制模式和单纯的回应模式，而应通过促使法律和技术在关照彼此核心价值诉求的基础上进行双重重构来实现和谐。通过法律与技术的双重重构重塑犯罪治理根基，一方面，需要区块链技术主动维护现有法律规制秩序，为外部监管的介入提供技术环境；另一方面，现行法律应对区块链技术的“去中心化”价值保持宽容态度，建立适应区块链发展需要的法律体系。此外，还要在法律和技术层面加强国际合作，减小区块链“分布式”特征对链上犯罪管辖的不利影响。

【关 键 词】区块链　智能合约　犯罪治理　双重重构

【作　　者】赵小勇，西南政法大学法学院博士生，西南政法大学特殊群体权利保护与犯罪预防中心助理研究员。（重庆 401120）

区块链是一种去中心化的基础架构与分布式计算范式，从比特币的出现到智能合约的运用，区块链技术的应用场景越来越丰富，被认为是计算范式的第五次颠覆式创新，其极有可能通过改变人们的交往和交易方式进而重塑整个经济社会发展形态，从而引起了政府部门、金融机构、科技企业等各行各业的高度重视与广泛关注。正是由于区块链技术构建起的交往空间与包括互联网空间在内的既有交往空间存在明显区别，最终可能致使传统犯罪治理模式难以承担区块链犯罪治理的重任。对此，我们应深入分析区块链技术运行机理，准确把握区块链技术的广泛运用给传统犯罪治理模式带来的危机，以促进法律与技术和谐共生为目标，思考区块链时代犯罪治理机制的革新。①

① 由于篇幅有限，本文讨论的区块链主要为具有普遍意义的区块链底层技术，对应的区块链运用类型主要为公链。

危机初现：区块链技术运用对传统犯罪治理根基的动摇

2016 年 6 月 17 日，黑客利用 The DAO 代码里的漏洞盗走了 360 万个以太币，直接导致以太坊硬分叉，尽管之后黑客还在网络上接受过采访，但至今人们仍然不知道黑客的真实身份。2018 年 1 月 25 日，日本最大的比特币交易所 Coincheck 遭到黑客攻击，损失高达 5.3 亿美元，之后虽然一些被盗的比特币在加拿大和日本的交易所被追查到，但仍然无法追回这些被盗的币。这些利用区块链实施的犯罪活动无法被追责，凸显了传统犯罪治理手段在这些犯罪面前的乏力，区块链技术环境下犯罪治理事业面临的深刻危机正暗含于此。

（一）“去中心化”对责任主体概念的消解

所谓责任，“就是意志形成的非难可能性”[①]，是“按照对一种行为或其结果的预期而追溯原因的关系系统”[②]。包括法律和道德在内的行为规范只有通过相应的责任机制才能发挥自身的规范作用。在我们通过责任来治理社会时，一个重要的前提是确实存在为结果承担责任的责任主体。在传统的犯罪治理过程中，也可能出现犯罪结果难以归属到特定主体的现象，但这往往只是追责技术不够先进的问题，而不是犯罪结果背后的责任主体存不存在的问题。但是，区块链的“去中心化”特征消解了传统犯罪治理中的“责任主体”概念，导致区块链环境下出现违法犯罪活动时，只有活动及结果本身，却没有为活动和结果负责任的主体，这对现有犯罪治理机制的挑战是致命的。

在区块链这样一个分布式系统中，虽然从整体上看，记载着交易往来信息的总账本只有一个，但创建并维护这个账本的工作却是由多个节点共同完成的。区块链“去中心化”的目的是通过记账权利（或义务）主体多元化、特定交易信息记账权确定的随机性和账目验证及保存主体的多元化等方式来实现。所以，区块链的运作是没有中心化组织负责的，而是由所有的节点（参与者）共同负责整个系统的运行和更新，不存在一个为分布式账本记录行为负责任的明确主体。这与传统互联网交易中由可信赖的第三方处理交易双方的往来账目完全不同。如前文所述，传统的犯罪治理中确定责任和责任主体至关重要，没有为危害后果负责任的主体，则传统犯罪治理制度就有坍塌的危险。而“去中心化”使得在区块链中不存在一个为违法犯罪行为负责任的明确主体，因此，我国现行刑法中诸如拒不履行信息网络安全管理义务罪等罪名，在区块链中就没有适用对象，现有网络犯罪治理体系在区块链环境中就出现“失灵”的现象。

（二）“匿名性”对传统归责路径的阻塞

上文指出在区块链上没有为区块链运行结果负责的责任主体，但是依据我们治理互联网的经验，我们会很自然地提出将区块链上的活动归属于参与区块链运行的现实世界中的主体的追责思路。确实如此，在传统互联网犯罪治理中，通过实名制可以将网络用户的身份与其个人真实身份信息建立一一对应关系，进而将网上活动归责于现实中的主体。

然而，在区块链时代，即使在事实上确实是由链下的主体组织实施了链上的违法犯罪活动，但由于区块链的“匿名性”（或称“假名性”）特征，传统犯罪治理手段很难从链上追溯到链下的这些主体。中本聪在提出比特币构想时就考虑到了交易信息公开对用户隐私的影响，但其解决思路不是对链上被公开的信息内容进行去隐私化处理，而是通过假名机制隐藏公开信息最终在现实世界中的归属。虽然目前通过大量分析交易和网络数据，可以设计去匿名方案，但即使这样，在目前的区块链上确定交易者的真实身份也不是一件容易的事。在前文提到的 The DAO 盗币事件中，虽然人们事后查到被盗以太币的交易记录，但至今都无法找到盗币的黑客。而随着新型的拟态防

① 汉斯·海因里希·耶赛克、托马斯·魏根特：《德国刑法教科书》上册，徐久生译，北京：中国法制出版社，2007 年，第 549 页。

② 汉斯·兰克：《什么是责任？》，《西安交通大学学报》（社会科学版）2011 年第 3 期。

御技术、网络层数据混淆技术、数据失真技术等的运用，区块链的“匿名性”程度将会变得越来越高。由此可以看到，区块链“匿名性”将世界截然划分为链上和链下两个部分，除了用户本人，其他人难以将两个世界对应起来，这一特征最终阻碍了对链上犯罪活动的追责，这是区块链时代犯罪治理面临的又一挑战。

（三）代码自动执行对外部力量介入犯罪过程的排斥

在现实世界和传统网络世界中，行为或网络活动的实施依赖于行为人或中心化组织（如社交平台、网购平台等）。在这些由人和中心化组织启动、参与的活动中，活动的发起者及参与者有多个中止或终止活动的时机，监管部门或犯罪调查部门等外部力量也可以较为容易地介入到活动过程中。在这些环境中，犯罪活动是可以基于犯罪行为人自己的意愿或外部力量的干预被中止或终止的。将违法犯罪活动消灭在萌芽状态或危害结果尚未发生的阶段正是传统犯罪治理的重要目标之一，为此现有刑法体系专门设置了犯罪中止及犯罪未遂制度。

随着区块链技术从 2.0 阶段走向 3.0 阶段，“代码法律化”与“法律代码化”两种趋势交织，人们积极探索将更多类型的实体合约表达在区块链代码中，通过智能合约的自动执行、不可篡改等技术特征为合约执行奠定了信任基础。但正因为“智能合约的所有条款和执行过程都是预先制定好的，一旦部署运行，合约中的任何一方都不能单方面修改合约内容以及干预合约的执行”，[①] 所以一旦智能合约本身存在的漏洞被用来实施违法犯罪活动，则无论是合约的开发者、合约当事人或外部的监管机构都无法中止或终止合约的运行。这就导致犯罪中止及犯罪未遂制度在区块链环境中，缺少对犯罪活动及犯罪分子发挥作用的空间。在犯罪活动事中干预机制失灵的情况下，如何通过健全区块链代码运行的事前及事后介入机制，限制其可能造成的违法犯罪后果，这也成为现有犯罪治理体系必须要解决的难题。

① 贺海武、延安等：《基于区块链的智能合约技术与应用综述》，《计算机研究与发展》2018 年第 11 期。

（四）“分布式”特征对网络空间主权管辖的削弱

当前，网络空间主权理论为我国对网络空间进行治理提供了理论基础与正当性。依据网络空间主权，国家对网络空间进行司法管辖的具体路径为：首先，针对网络设施适用“领土原则”。对于网络设施，无论由国家、组织或个人所有，都应依循领土原则处于国家管辖之下。其次，针对网络主体，适用“国籍原则”。由于网络空间的虚拟性，网络主体的地理位置往往难以判断，但通过信息技术和线下配合却容易获得其真实身份，并由此成为确定管辖权的重要方式。最后，针对网络行为，可适用“效果原则”。无论网络行为是否在一国领土之内，只要它在领土之内产生或意图产生不利影响，均在该国的管辖范围内。[②]

② 参见张新宝、许可：《网络空间主权的治理模式及其制度构建》，《中国社会科学》2016 年第 8 期。

但是在区块链环境下，上述关于网络空间司法管辖路径的理论就变得不再可行：首先，区块链的节点全球分布，即使根据“领土原则”对分布在我国的节点进行管辖，但由于只有多数节点取得共识才能对区块链运行规则及结果进行改变，所以只对分布在我国的区块链节点进行管理，对整个区块链网络来说是“无关痛痒”的。其次，由于区块链的“匿名性”，可能无法或者很难根据“国籍原则”通过信息技术和线下配合确定网络主体的真实地理位置和身份。最后，由于区块链网络很难说位于哪国领土范围内，所以即使区块链上发生了违法犯罪结果，也很难根据“效果原则”，主张链上的违法犯罪效果发生在我国领土范围内。由此可见，对区块链“分布式”特征带来的挑战，如果我们不能进行有力回应，会直接动摇我国立法所坚持的网络空间主权立场，破坏我国网络犯罪治理的立法基础。

双重重构：区块链时代法律与技术的和谐共生之道

上述所言区块链技术的运用对传统犯罪治理带来的挑战，说到底是区块链技术构建的交往方式突破了原有法律调整社会关系的固有模式，造成了区块链技术与法律规范之间的紧张冲突。自近代以来，妥善处理法律与技术之间的关系已成为人类社会发展过程中面临的一个重要主题，人类社会对此已有诸多思考和实践。在思考如何促进法律规范与区块链技术和谐相处这个问题的时候，不妨从已有的法律与技术关系模式理论及我国技术治理实践出发，做一番考察。

（一）法律与技术的关系模式

P. 诺内特和 P. 塞尔兹尼认为，社会上存在的法律现象可以分成三种类型：压制型法、自治型法以及回应型法。[①]郑玉双借鉴了这一划分理论，提出将法律与技术之间的关系模式划分为管制模式、回应模式和重构模式三种。其中，管制模式是指法律将技术视为实现特定社会目标的工具，技术只具有工具价值。如果技术适用有利于社会发展，那么就通过法律对技术适用进行保护，如果对社会不利，则需要通过法律进行压制。回应模式的重点在于法律在回应技术发展和社会冲突中所体现出的自我调整机制，即不把技术的社会意义当作压制和驯化的对象，而是通过回应来安置技术的社会意义和潜在的价值冲突，弱化了法律要求服从的义务。重构模式则主张将技术价值与法律价值纳入一个重新评估和衡量的语境之中，一方面包含对技术社会价值的解释，另一方面体现为将技术纳入法律规范的意义结构之中。[②]

可以看出，管制模式中法律面对新技术带来的挑战，拒绝对自身做任何调整，强势地要求技术以适应原有法律规范为目的作出单方面调整。而回应模式虽然面对新技术展现了柔和的一面，并在现有法律框架内对新技术的发展需求给予回应，但这种回应“是建立在对技术价值的肯定的基础上，并不包含道德论证的方案和框架”[③]。重构模式虽然也和回应模式一样，有顺应技术价值进行自我调整的一面，但重构模式对技术发展的此类“回应”同时是带有批判性的，即“整体性的法律方案将技术价值通过社会结构的过滤器纳入到法律的价值论辩之中”[④]。而这种批判性回应的结果，最终要求技术也必须在一定程度上回应法律价值的需求。

（二）我国网络治理实践对法律与技术关系模式的检验

1. 对抗 = 灭亡：回应模式及管制模式在我国治理 P2P 网络贷款中的运用

近年来，我国对 P2P 网贷的治理模式经历了从宽容鼓励到严厉整顿的立场转变，这背后体现着法律与技术关系的不同模式，为我们观察不同关系模式处理法律与技术冲突的效果提供了生动的实践样本。

回应模式阶段（2007—2015 年）：P2P 网贷在 2007 年从国外传入中国，2013 年后开始在我国获得迅速发展。在整个互联网金融发展初期，P2P 网贷对普惠金融理念的践行、对中小微企业融资难问题的缓解以及对个人消费信贷的促进作用被法律及政策充分肯定。由于对其运作模式及蕴含的风险认识尚不充分，监管层面对包括 P2P 网贷在内的互联网金融采取了较为宽容甚至倾向于鼓励的态度。但随着 P2P 平台越来越多，行业资金规模越来越大，一时间数百家 P2P 平台陷入非法吸收公众存款、集资诈骗等丑闻，涉案资金动辄数十亿元，受害人往往遍及多个省份。

管制模式阶段（2016 年至今）：2016 年前后，随着国家对 P2P 网贷行业的风险状况越来越担忧，监管态度逐渐转变为对 P2P 网贷进行严厉整顿。其间，国家监管部门围绕整顿互联网金融风

① 参见 P. 诺内特、P. 塞尔兹尼克：《转变中的法律与社会：迈向回应型法》，张志铭译，北京：中国政法大学出版社，2004 年，第 85、87、57、127 页。

②③④ 郑玉双：《破解技术中立难题——法律与科技之关系的法理学再思》，《华东政法大学学报》2018 年第 1 期。

险密集出台多个规范性文件，直接为 P2P 网贷的运作划定“红线”，超出“红线”的平台一律关停，其间更有多个省份直接出台“一刀切”的政策，清理掉辖区内的所有 P2P 网贷平台。严厉整顿之下，全国 P2P 平台数量自 2017 年的 2000 余家骤降至目前的 20 余家。①

我国治理 P2P 网贷的历程，给我们治理区块链环境中犯罪问题的启示是：第一，回应模式虽然展现了法律和政策对新型技术宽容的一面，为新型技术留足了发展空间，但这种模式如果不能及时有力回应新型技术本身存在的风险，仅仅是展现宽容的一面，则新型技术可能走向失控的境地。此时，对技术的规制不得不走向管制模式。第二，如果新型技术在发展的过程中，不注意从技术运行机理层面主动遏制自身所具有的破坏性力量，则其极有可能在较为宽松的规制环境中走向失控，彻底失去被法律信任的机会，从而被全面限制和整顿。第三，在法律政策与技术的二元关系中，同样遵循“合则两利、斗则两败”的博弈逻辑，对抗就等于灭亡，这是新型技术野蛮发展面对强硬法律监管的必然下场。由此可以看到，运用回应模式和管制模式处理法律与互联网之间的关系，效率与效果都不够理想。

①《郭树清称网贷已至根本性转折点，目前仅剩 29 家网贷平台在运营》，界面网，https://www.jiemian.com/article/4826697.html，2020 年 8 月 15 日。

2. 以退为进：双重重构模式在网约车治理过程中效果的彰显

如上文所述，重构模式实质上要求法律和技术互相进行回应、调整，所以本文认为，将这种模式称为法律与技术的双重重构关系模式更为准确，即重构中既要强调法律的重构，也要强调技术的重构。

在我国近年技术治理的实践中，对网约车的治理体现了法律与技术的这种双重重构的形态。我国政府对网约车的治理经历了观望阶段、取缔阶段和监管阶段三个时期。②在监管阶段，行政法规改变了在取缔阶段认为网约车非法的态度，而将其纳入监管范围，并对其安全性提出要求，促进其与传统出租车行业良性竞争。而网约车行业也积极回应监管要求，加强对网约车及其车主的管理，不断优化运行模式并加大科技投入，主动防范网约车运行中车主侵犯乘客权益等违法犯罪现象。如今，网约车行业日渐成熟，网约车已经成为社会大众日常生活中的常见出行方式。我们看到，正是由于法律政策与网约车各自在回应对方核心价值关切之后主动进行自我调整，才最终实现了两者的和谐共生、互相成就。

② 参见范永茂：《政策网络视角下的网约车监管：政策困境与治理策略》，《中国行政管理》2018 年第 6 期。

从我国治理网约车乱象的历程中，我们可以看到双重重构模式的运用需要具备以下几个条件：第一，冲突中的法律与技术的核心价值诉求点本身是不同的。如果法律和技术的核心诉求点是同一个问题，则会将法律与技术推向“不是你死，便是我亡”的“零和博弈”境地，两者从根本上缺乏对话协调的可能，从而各自也就没有进行重构的基础。第二，双重重构需要抛弃法律中心主义而改采“法律–技术”二元互动模式。即需要重构的不只是技术体系，还有法律体系，不仅是法律要求技术做出调整以适应法律秩序，技术也反过来要求法律做出调整以适应技术的发展需要。第三，双重重构的目标是通过法律与技术在价值诉求上相互妥协得以实现的。这种妥协需要法律与技术各自放弃自身对非核心价值的诉求以换取对方的生存空间，同时各自坚守自己的核心价值诉求以保存自身的主体性和独立性。概言之，在双重重构中，法律与技术以相向而行的态度“各退一步”，分别对各自非核心价值诉求进行限制，最终实现法律与技术的和谐共生。

（三）走向双重重构——法律与区块链关系模式的应然选择

我国互联网治理实践表明，在法律与互联网技术的几种关系模式中，双重重构模式最具生命力，能够从根本上解决法律与技术之间的紧张冲突，取得法律价值与技术价值的共赢。但这是否

就意味着在构建法律与区块链技术之间的良性关系以实现区块链犯罪的有效治理时，也必须要采取双重重构模式呢？本文认为答案是肯定的，理由如下。

第一，除非得到区块链技术的响应，否则区块链的自治特性将彻底排除法律对区块链进行干预的可能。区块链技术的产生源于对现有中心化组织的不信任，拒绝法律对区块链运行的干预本就是区块链技术追求的重要目标，这与我们熟悉的互联网环境完全不一样。面对既有自治意愿、又有自治能力的区块链，在未唤醒技术层面为回应法律秩序进行主动的自我改造之前，即使法律体系对区块链实施单方面压制或单纯的回应，区块链也可凭其“匿名性”、“去中心化”、运行过程拒绝外部介入、节点全球分布等机制将来自法律的各种干预化解于无形，在这种情况下区块链环境中的犯罪治理便无从谈起。所以运用法律对区块链进行有效治理，需要区块链技术体系以适应法律监管为目标进行技术重构为前提。

第二，除非得到法律体系的支持，否则区块链技术将在较长的时期只能在狭小空间实现其自治运行的梦想。区块链渴望自立于法律体系之外运行，但遗憾的是，至少在目前，法治仍然是国家治理的基本方式，是国家治理现代化的重要标志。法律面对区块链运行中可能出现的违法犯罪这一“负外部性”不可能无动于衷。如上文所述，如果法律此时选择对区块链技术进行强力压制，虽然区块链可以无视来自法律的限制继续以自治的方式运行，但区块链在人类生产生活中可以发挥作用的范围必然大为压缩。换言之，在法律仍然为国家及社会治理的根本凭借时，区块链技术只有获得法律体系的善意对待，才可能在更大范围、更多方面实现技术价值，而这需要现有的法律体系以适应区块链技术发展需要为目的进行自我重构。

转危为机：以双重重构模式重塑区块链时代犯罪治理基础

（一）区块链技术的重构：为监管介入提供技术支持

区块链技术的运用对犯罪治理造成的责任主体概念的消解、归责路径的阻塞、介入犯罪过程困难及司法管辖的弱化几个障碍，最终阻碍了外部监管对区块链运行过程的介入，使得原有犯罪治理中的一切追责活动都无法进行，法律在区块链犯罪治理中的价值就此被大为削弱，这是现有法律及政策的“不能承受之重创”。重构区块链技术，就是要从技术层面降低监管障碍，为法律监管介入区块链运行提供技术支持。这一重构工作至少可以从以下几个方面进行。

第一，实现高度“匿名性”向“可控匿名性”的转变。在区块链技术给犯罪治理带来的障碍中，“匿名性”对法律监管造成的影响是最为“伤筋动骨”的。但“匿名性”本身却并不是区块链技术的核心价值诉求，区块链技术至少可以放弃对绝对“匿名性”的追求。因为区块链最核心的“去信任”价值诉求是通过去中心化、分布式、工作量证明和不可篡改性实现的。区块链技术担忧的用户隐私问题，其实只要区块链放弃对绝对“匿名性”的追求，使监管层面能够掌握各节点的真实身份，则一旦有人在区块链上通过技术手段侵犯用户的隐私权，则法律就可以通过实名机制找到现实世界中的侵权主体，追究其相应的法律责任，这一过程与传统互联网中法律对隐私的保护机制大体相同。在技术层面已有信息工程方面的学者提出区块链中“‘前台自愿、后台实名’的可控匿名性”概念，并提出“要在可监管的基础上实现用户的隐私保护”[①]。当前国内外网络安全学者都已经在此方面有了相关的技术研究成果，[②]虽然目前实现区块链“可控匿名性”的技术尚不成熟，但这应该成为鼓励支持的区块链技术发展方向。

① 付烁、徐海霞等：《数字货币的匿名性研究》，《计算机学报》2019年第5期。

② 姚前：《中国版数字货币设计考量》，《中国金融》2016年第12期；李佩丽、徐海霞：《区块链用户匿名与可追踪技术》，《电子与信息学报》2020年第5期。

第二，完善智能合约运行的技术约束环境。虽然智能合约的运行确实可能带来违法犯罪的结果，但由于智能合约一旦部署就不可篡改，并自动运行，所以区块链技术在此处的重构只能着眼于在智能合约上链前及运行后的阶段进行技术改进。一是构建代码审计机制。在开发、测试和上线等阶段就由独立于开发者的主体对代码的漏洞进行审计，对代码的安全性进行评估，通过审计将智能合约可能存在的安全隐患消除于源头，防患于未然。智能合约代码审计既要关注代码与参与者的意思表示是否一致，也要关注代码本身的运行安全，将代码经过审计验证作为智能合约上链的前置条件，将审计信息与智能合约同时上线，以此最大程度地保证上链智能合约本身的安全可信。二是对智能合约漏洞构建回滚交易机制。“通过使用基于事务的数据回滚机制，数据库管理系统可以将数据恢复到某一时刻的一致性状态。目前的区块链系统虽然具有信息不可篡改特性，但依然可以通过硬分叉的方式实现数据回滚的功能。”[①]但由于回滚交易实质上构成了对智能合约运行结果的篡改，频繁运用回滚交易会削弱智能合约的受信赖程度，所以对其进行的运用必须被限定在一定范围内。对此，在智能合约代码中嵌入回滚交易机制时，应对触发回滚的包括严重违法犯罪在内的异常事件进行精心设计，从而将智能合约回滚限制在一定范围内，以最大程度维护智能合约的可信赖性。

第三，在区块链中设置监管节点。“匿名性”将区块链隔离为链上与链下两个世界，致使位于链下世界的犯罪治理部门难以掌握链上违法犯罪活动的情况，缺乏介入链上活动的渠道。但是在链上空间，区块链的运行状态却是公开透明的，且每一个节点都能参与区块链的运行。于是，信息安全学者提出了“以链治链”的区块链监管思路，即“在不同类别的区块链网络体系中，纳入监管节点，以全局视角对区块链网络内所有的区块链进行强有力地全方位监管”[②]。通过设立监管节点，一方面监管部门可以实时掌握链上各种活动，及时发现违法犯罪现象。另一方面，通过为监管节点赋予更大的权限，使监管部门在参与区块链运行的过程中拥有更大的决策权重，以便有效阻止区块链上违法犯罪活动的出现。

（二）法律的重构：构建与区块链技术特征相适应的法律规范体系

如前文所述，对于区块链来说，“去信任”才是其最核心的追求，而这主要是通过“去中心化”“分布式”等来实现的。因此，区块链技术即使可以在“匿名性”问题上作出让步，但其无论如何也无法在“去中心化”“去信任”等方面作出让步。所以，法律的重构就不能采取管制模式强迫区块链技术在“去中心化”方面作出改变，而是应考虑在法律内部调整现有运作模式，构建与“去中心化”“去信任”特征相适应的新的法律规范体系，如此方能保证将犯罪治理力量有效投送到区块链环境中去。

首先，构建基于节点的法律责任体系。在区块链中，传统网络平台对网络活动的管理职能被分散给了链上的所有节点。权力与责任是相统一的，既然传统平台的监管职能被分散给了链上的所有节点，那么我们完全可以考虑立足于这些节点，建立区块链环境下的新型法律责任体系。事实上，我国监管部门已经在此方面迈出了实质性的步伐，国家互联网信息办公室于 2019 年 1 月出台的《区块链信息服务管理规定》明确规定，“向社会公众提供区块链信息服务的主体或者节点”具有对平台进行管理、接受配合监管及不得利用平台实施违法犯罪活动等义务，对违反这些义务的行为规定了追究行政责任和刑事责任等多种处罚措施。但这些规定当前还显得较为粗糙，“其中一些概念的具体含义并不明确，需要展开法律层面的探讨和解释”[③]。而且在区块链技术没有完成技术重构的情况下，基于节点的法律责任体系仍然将面临无法在现实世界中找到责任主体的

① 于戈、聂铁铮等：《区块链系统中的分布式数据管理技术——挑战与展望》，《计算机学报》2019 年第 10 期。

② 邹萍、李艳东等：《区块链监管的现状与展望》，《网络空间安全》2019 年第 6 期。

③ 贾翱：《区块链信息服务监管对象研究——以〈区块链信息服务管理规定〉第二条为中心》，《大连理工大学学报》（社会科学版）2020 年第 2 期。

困境。所以，区块链技术重构与法律重构必须同步实施，只有在“可控匿名性”和监管节点的加持下，基于节点的法律责任体系才能发挥好对违法犯罪的追责功能。

其次，解释性构建适用于区块链环境的罪名体系。区块链改变了人类社会的信任机制，实现了“去信任”，这意味着现有法律中一些以保护和促进信任为目的的具体制度，可能难以直接适用于区块链环境。比如，传统诈骗犯罪理论认为，构成诈骗罪的前提条件之一是在行为人的影响下使“被害人陷入错误认识”。但是在智能合约中，合约内容及其运行方式在事先已经以代码的形式完全展示给了参与者，如果参与者未能发现合约中的“陷阱”，参与合约遭受损失，显然不属于被害人在行为人的欺骗下“陷入错误认识”，此时说被害人“被骗”可能就站不住脚，主张行为人构成诈骗罪就有问题。显然，传统诈骗罪的犯罪构造应进行重新解释，有必要考虑将“被害人陷入错误认识”条件剔除出诈骗罪的犯罪构造。此外，关于区块链中代币在刑法中的性质归属问题，也需要对刑法中的“财产”“利益”等概念进行重新解释。总之，我们需要根据区块链对人们交往方式的改变，系统性地对刑法中的一些概念重新作出解释，构建起一套能够有效规制区块链上犯罪活动的罪名体系，为区块链时代的犯罪治理提供有力支撑。

最后，探索推动与“代码法律化”趋势相呼应的“法律代码化”。代码在区块链中形成规则、调整人们之间关系的过程，可以视作一个制定法律规范的过程，这意味着法律可能在一定程度上能够以代码化的方式存在，于是便形成“法律即代码”（law is code）的概念。对此我国有学者进一步指出，“法律将代码化，即将法律通过代码加密，通过数字化形成一个交易规则、交易过程。否则，目前的法律体系和法律监管体系、规则的执行体系是无法适应人工智能时代发展趋势的”[①]。“法律代码化”虽然随着智能合约的运用已然开始，但国内法律对哪些领域的法律可以代码化，法律代码化过程如何进行规范，代码化后的法律及其运行的效力如何确定，立法层面是否要主动适应代码化要求等问题，尚缺乏思考。而国外的法律及计算机学者已经对此展开研究，比如有国外学者从“安全港条款”“沙盒监管”“合约模块化”等方面观察“法律代码化”。[②]随着我国区块链及智能合约的发展，为“法律代码化”立“规矩”，将成为法律体系从根本和源头上预防区块链犯罪的一项重要举措。

（三）全球治理的提倡：加强区块链技术治理的国际合作

对全球性问题的治理单凭一个或一些国家的行动难以取得理想效果，虽然通过国际合作来解决这些问题效果也仍然有限，但这终究是相对最优解。对区块链环境下的犯罪治理也只有通过加强国际合作的方式，才能取得比一国“单打独斗”更为理想的效果。这一合作可以从两个层面开展：其一，从法律的层面加强合作，基于刑事犯罪普遍管辖原则和刑事司法协作机制，在区块链技术的法律规制方面形成合力，化解区块链节点全球分布带来的链上违法犯罪的治理难题。其二，从技术的层面加强合作，共同构建区块链技术和运用的安全标准。比如，推动各国就区块链实名制或可控匿名技术、区块链监管节点的设置等问题达成共识，实际上目前有多个国家已经在网络空间推行可信身份战略。我们有必要将各国应对区块链技术挑战的努力联合起来，如此才能在全球治理的框架下，从技术和法律两条进路共同探索出区块链时代犯罪的全球治理之道。

编辑　杜运泉　孙冠豪

① 关仕新：《法律代码化以适应人工智能发展》，《检察日报》2017年11月23日，第3版。

② 凯文·沃巴赫：《信任，但需要验证：论区块链为何需要法律》，林少伟译，《东方法学》2018年第4期。