规则与技术之间：区块链技术应用风险研判与法律规制

金　璐

（广西民族大学法学院　广西南宁　530006）

内容提要：区块链作为智能互联网时代的核心驱动力，在给人类的生产和生活方式带来巨大变革的同时，亦存在着技术规制短板和法律规制困境。区块链技术应用“犯规”主要体现为共识算法安全和效率提升的现实悖论、智能合约的漏洞风险、信息技术权利的滥用风险以及技术规范的价值局限。对区块链技术应用风险的法律规制是我们在全面迎接“代码法”和“数字治理”时代的重要制度预演，具有现实而迫切的意义。法律对区块链技术应用风险的规制应遵循激励规制原则、创新规制原则以及区别化规制原则的法治指导。对智能合约漏洞风险我们应创新规制方法，打造多方配合协同共治的格局；对权利滥用的失范需遏制传统问题升级演化，亦需强化对新问题的规制；算法风险的化解有赖于技术性应对策略并使技术助力法律的实施。除此之外，调适抑制负效应的法律机制也是十分重要的，有助于实现区块链技术的价值形塑。

关键词：区块链技术　技术应用风险　法律规制

DOI:10.16092/j.cnki.1001-618x.2020.07.010

“区块链”技术是继移动互联网、大数据、云计算、人工智能后又一历史里程碑式的技术创新，它开启了共享经济新时代，引领着全球技术及产业变革。2019 年习近平总书记在两院院士大会上强调：“以……区块链为代表的新一代信息技术加速突破应用……，科学技术从来没有像今天这样深刻影响着国家前途命运……”[①]作为新型互联网技术，区块链在建立信任关系、提高协作效率、促进数据共享、提升政府穿透式监管能力等方面具有不可替代的作用，[②]“我们要把区块链作为核心技术自主创新重要突破口，加快推动区块链安全有

作者简介：金　璐（1987—），女，汉族，浙江杭州人，广西民族大学法学院讲师。

本文为 2018 年度广西民族大学研究生课程建设项目（项目编号：gxun－chxkc201809）和广西民族大学人才引进项目（项目编号：2016MDRC004）的阶段性成果。

① 习近平：《在中国科学院第十九次院士大会、中国工程院第十四次院士大会上的讲话》，http://www.xinhuanet.com/2018－05/28/c_1122901308.htm，访问日期：2020 年 1 月 2 日。

② 工业和信息化部信息中心：《2019 年中国区块链产业白皮书》，第 45 页。

序发展。”[③]在这一背景下展开区块链应用中的法律规制研究，对我国探索共享经济新模式、建设数字经济产业生态、提升政府治理和公共服务水平具有重大而深远的意义。

一、区块链技术风险引起的混乱

（一）算法安全隐患

在技术层面，区块链数据有赖于区块链算法规则。算法规则是根据密码学算法将区块按时间顺序连接成链的数据结构：共识算法使区块链系统上各节点达成一致，实现数据写入的安全性与合法性；摘要算法使得长短不一的信息都以固定长度输出，保障数据的完整性；加密算法对数据进行密码变换而产生密文，用于实现读取数据的安全性。[④] 上述算法不但使得区块链系统内各区块之间相接连贯，身份验证准确，还保持了信息数据的完整性。虽然算法在理论上得到了应用支撑，但当前技术安全机制仍有待提升，其存在来自区块链系统内部和外部的算力攻击，威胁区块链系统安全。算力攻击是区块链系统上的节点利用自身的强势算力在系统内节点的算力角逐中胜出并对既往数据记录进行不法操作的行为。在工作量证明方式（PoW）的共识算法中，存在“少数服从多数”规则。这意味着如果节点计算力强于系统其余算力便可任意控制和处分数据信息。故节点越多，区块链系统的参与者依靠强势算力篡改或伪造数据的难度就越大，区块链系统的安全性和公平性也就越高。区块链系统外部同样存在量子计算的算力攻击。量子计算作为一种新型计算方式，遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息。有专家预测，在不远的将来量子计算能够轻易破解基于加密算法构建起来的网络系统。[⑤] 算力攻击一旦顺利达成，轻则可以通过窃取节点账户信息（如私钥等）给有关区块链参与者造成难以弥补的财产损害和隐私泄露；重则凭借超强算力通过篡改大部分节点账户数据控制整个区块链系统，挑战国家网络安全和信息安全、金融安全等领域，威胁国家主权、民生福祉及社会稳定。

区块链技术还存在安全与效率顾此失彼的技术短板。当前技术的数据吞吐量和存储带宽能力暂时难以满足大多数网络用户的数据处理需求量。在信息大爆炸的今天，大频次、大资金的交易场合将是对区块链技术性能的极大考验。由于一条记录需要大多数节点的区块确认方能生成，故节点基数越大该条记录达成共识所需的确认时间越长。节点数量的增多固然会提升区块链系统的安全性，但同时也降低了区块链系统的效率，故算法安全和效率提升成了“鱼和熊掌不可兼得”的现实悖论。

（二）智能合约存在安全漏洞

区块链下的智能合约存在技术性结构安全漏洞，进而导致智能合约当事人遭受财产损失，但因缺乏有关法律规范而无法获得有效救济。在四类主要的区块链安全事件（即共识机制、智能合约、交易平台及用户自身安全事件）当中，因智能合约漏洞引发的事件遭受的损失最

③ 《习近平在中央政治局第十八次集体学习时强调把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展》，http://www.xinhuanet.com/politics/leaders/2019-10/25/c_1125153665.htm，访问日期：2020年1月2日。

④ See Caryn Devins, Teppo Felin, Stuart Kauffman, Roger Koppl. The Law and Big Data Cornell J. L. & Public Policy, 2017.

⑤ See Elizabeth Gibney, Physics: Quantum Computer Quest, Nature, 516, 24-26, 04 December 2014.

为严重。[6] “智能合约是运行在计算机系统上，事先设计好的一个合约执行程序，当一定条件被满足时，可被触发进而自动执行的合约形式。”[7]意思表示、合同法定构成要件、当事人履约均是传统合同必不可少的核心要素，而智能合约是不以传统合同法定构成要素为依托的特殊合约，具有去中心化、自动执行的特征，会导致现有法律体系对其界定困难，既无法将其归为一般的财产构造，又难以认定其为严格的合同构造。简言之，由于缺乏对区块链系统及其内部关系性质的明确界定，[8]在智能合约和传统合同法之间存在一种技术与法理的羁绊。对于区块链信息服务提供者来说，若要对智能合约漏洞进行有效防范，当事人基于智能合约不可修改的特征，只能选择重新编写新的智能合约的方式，但这将以金钱和信誉损失为代价，故其往往以一种“怠于响应”的消极态度来应对这种技术与法理之间的矛盾。这将导致公众无法对技术安全秩序建立起应有的稳定预期。

此外，由于缺少及时核查和修复的有效机制，智能合约存在技术结构性安全漏洞。技术性结构安全漏洞包括源代码漏洞、业务逻辑漏洞等计算范式中的技术漏洞。这些漏洞会导致合约运行的不法结果，甚至是无法弥补的损失。无论是 The DAO 众筹项目中的智能合约[9]还是美链 BEC 智能合约，[10]抑或是以太坊智能合约[11]都发生了漏洞导致巨大财产被非法转移的重大事件，智能合约俨然已经成为区块链安全的重灾区。智能合约是一把双刃剑，在解决交易信任问题的同时又会滑落到去中心化智能合约系统的陷阱中。然而，就制度规范而言，虽然《区块链信息服务管理规定》（以下简称《规定》）第 6 条规定：“区块链信息服务提供者应当具备与其服务相适应的技术条件，而且技术方案应当符合国家相关技术标准规范”，但关于智能合约结构性问题的法律规制尚付阙如。对于区块链安全性能，研究者同样面临左右为难的尴尬境地，如若公布漏洞细节将会对信息服务提供者和部分系统用户的数据安全不利，但不披露则会加剧网络黑客不法攻击的频率，削弱供应者的系统安全意识，致使更多系统用户遭受利益损失。

（三）区块链信息技术权利的滥用风险

作为新兴信息技术的区块链塑造了新型信息社会，但是对新技术缺乏应有的法律规制会放任信息技术的滥用，可能使信息社会的结构异化，形成社会被技术反噬的态势。首先，区块链技术下信息服务提供者可以从事任何交易且绕过银行等金融机构的交易监管，进而成为毒品交易、赌博、洗钱、盗窃甚至是恐怖活动和国家间谍活动等的法外乐土。针对区块链信息技术权利被滥用的风险，《规定》第 10 条已经明确作出限制权利滥用的规定。[12] 然而在现实网络中，有关部门很难精准高效地追踪犯罪痕迹。

⑥ 从事件损失金额来看，交易平台事件占据所有安全事件损失总金额（28.64 亿美元）的 46.93%，智能合约安全事件占据 43.3%，用户安全事件占比 8.25%，共识机制安全事件占比 1.08%。从安全事件发生频率来看，交易平台发生的安全事件占据所有区块链安全事件总量的 56.67%，用户安全事件次之占比 25%，智能合约安全事件占比 6.67%，共识机制事件约占 3.33%。

⑦ 马昂、潘晓：《区块链技术基础及应用研究综述》，载《信息安全研究》2017 年第 11 期，第 971 页。

⑧ 汪青松：《区块链系统内部关系的性质界定与归责路径》，载《法学》2019 年第 5 期，第 130 页。

⑨ 参见王化群：《智能合约中的安全与隐私保护技术》，载《南京邮电大学（自然科学版）》2019 年第 4 期，第 64 页。

⑩ 参见赵伟：《基于符号执行的智能合约漏洞检测方案》，载《计算机应用》2020 年第 4 期，第 949 页。

⑪ 参见王化群：《智能合约中的安全与隐私保护技术》，载《南京邮电大学（自然科学版）》2019 年第 4 期，第 63 页。

⑫ 《规定》第 10 条：“区块链信息服务的提供者和使用者不得利用区块链信息服务从事危害国家安全、扰乱社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动。”

即便能够追溯到犯罪交易详情，但由于区块链信息服务参与者的匿名性，有关部门也很难发现真正的责任主体。其次，跨越国界的区块链技术信息服务尚缺乏国际范围内打击犯罪的共同机制和准则，国际司法协助的有关制度安排阙如。这会导致在打击网络跨国犯罪中出现犯罪认定标准差异大、侦查机关的侦查和取证工作开展难度大、全球范围内受害者保护难度大的“三大”困境。再者，区块链技术可能会加剧“异型网络犯罪”的趋势，进而对信息网络环境的有序运行造成新的危机。区块链技术出现后，暗网交易可以完全摆脱中心化的传统金融监管机构，实现集封闭、不受实体控制和追踪、线下同步交易于一体的独立完整的网络系统。基于区块链技术的匿名性特征，系统的参与者往往关注于交易的实际内容，缺乏对参与者线下真实身份的考证，导致有关参与者冒用他人身份或者使用虚假身份在区块链从事不法活动。此外，区块链技术发展过程中存在区块链的伪应用及欺诈风险。区块链技术本身的去中心化并不意味着链上的应用服务也同样实现去中心化，现实中链上的应用服务可能依然是中心化的。区块链信息服务提供者可以直接通过中心化应用程序向终端用户发行加密代币，规避传统法律制度。不法之徒借着区块链技术投资的风口，披着“区块链”外衣行传销、诈骗、资金盘之实。区块链平台监管的严重缺失反映出区块链交易平台的中心化本质。区块链信息技术的催生不意味着能够完全避免或克服传统互联网中心化架构下存在的网络欺诈等老问题。

（四）区块链技术规范的价值局限

对技术进行约束的技术规范很大程度上被限定为工具理性而非价值理性，脱离价值理性而存在的工具理性存在内部的价值缺陷。技术的创造不受法律、道德等外部规范的制约，并且技术规则内部无法产生是非善恶的价值评判标准。在工具理性指导下，区块链技术的参与者几乎不会受到价值理性的约束，使得冷冰冰的技术规则大行其道，极易偏离善治、法治、德治的轨道。区块链技术理性带来的客观物化极有可能引发人类社会的道德危机。将外部价值的约束施加于区块链技术之上，并不是对“人的共识”和“机器共识”的混淆视听，因为后者不是自我创设、克制及完善的产物，而是人类智慧的产物。虽然上层建筑“人的共识”依托“机器共识”的基础，[13]但这并不意味着区块链技术就可以反客为主，拥有所谓“代码即法律”的权威和权力。区块链技术对于公平正义的实现在一定程度上具有理论和实践的双重瓶颈。区块链技术在规范区块链主体的实质平等性、开放性方面仍存在先天不足的问题。这种先天不足体现在区块链技术无法摆脱无处不在的“算力歧视”上。算力歧视一方面可以表现在区块链特定共识算法规则之上。Pow共识算法采取的是简单多数决原则，只要有所有节点过半的算力，便可任意控制区块链系统内的数据信息，形成算力的绝对话语权和对区块链系统内数据的支配权，因此拥有了攻击系统的能力。正义是不能通过剥夺少数人的自由使更多人分享较大利益来实现的。[14] 对算力的简单多数决的技术安排会置其他节点或集体的利益于不顾，进而出现对算力简单多数决的滥用。实践中，具有算力优势的“矿工”可以掌控更多的数据权利，数字货币交易所也可以凭借其在数字货币市场的资产管理者的地位拥有排他的区块链治理权

⑬ See Philipp Hacker, Ioannis Lianos , Geogios Dimitropoulos , Stefan Eich. Regulating Blockchain: Techno – Social andLegal Challenges. Oxford University Press, 2018.

⑭ ［美］约翰·罗尔斯：《正义论》，何怀宏等译，中国社会科学出版社2009年版，第12页。

力。另一方面，区块链算力歧视造成的“数字鸿沟”会带来技术利用或开放性问题上的不平等。算法精英基于技术优势会将其他阶层的人群排除在区块链经济和市场之外。算法的技术成果虽然可以通过提高透明度的方式确保算法的显性公平，但是技术固有的复杂性和知识产权保护的合法盾牌直接导致区块链技术不可能完全公开，区块链技术算法背后的隐形不平等问题无法彻底根除。区块链技术“仍然无法超脱社会化的情景预设，人性功利主义特质决定了区块链终究难以单纯依赖数据治理”。[15]

二、区块链技术应用“犯规”的治理逻辑

对区块链技术的风险治理可以为网络信息空间提供稳定安全的网络生态，同时，区块链技术也可以为法治提供治理的新理念和新面向。对区块链技术的风险治理应纳入法治化、规范化、制度化的轨道中。

（一）法治框架：应用风险规制的外在逻辑

对区块链技术应用风险的法律规制既要突出对新问题的规制，也要遏制传统问题的升级演化。互联网技术监管以维护网络安全为首要任务，以维护网络空间主权和国家安全、社会公共利益为主要目的。区块链技术在一定程度上有助于缓解传统互联网时代矛盾较为突出的个人信息保护、知识产权保护等法律急需回应和调整的问题，但是它也存在着与传统互联网技术伴随产生的网络犯罪等老问题，甚至演化为老问题的升级版。区块链系统的完全共享账本方式增加了交易透明度，却也未能摆脱用户隐私安全的传统网络风险隐患。在 2019 年“MIT 比特币世博会”上，会议现场向公众展示了物理密钥如何提取并攻击当前最安全的高科技数据加密存储器，快速窃取节点上所有的数字资产、历史交易记录等私人信息。老问题升级的同时也伴随着新问题的产生，而新问题植根于新型技术架构特征当中。去中心化、集体维护、全程留痕、共享账本等区块链技术特征可以保证区块链上的“诚实”与“透明”，有效解决传统经济社会信息不对称问题，实现多个主体之间的协作信任与一致行动。对这种颠覆性的网络架构进行行为规制和权利义务分配不宜完全照搬传统互联网信息技术下的有关规范。在网络空间中区块链交易者被化约为节点和数据，交易者的独立人格与主体形态难以准确识别。[16]现行立法关于这些主体形态缺乏法律定位和权利义务规制。对区块链智能合约等新型应用的技术性和结构性漏洞，以现有《合同法》应对不免显得捉襟见肘。

（二）技术规则：应用风险规制的内在逻辑

从系统功能看，区块链技术规则主要是通过系统内多方参与、协作、用算法传递和加固“信任”系统的方式防范区块链系统的安全风险，重点强化系统节点的“信任”，实现系统内部的“可控”。这主要体现在区块链系统采用节点身份可知的准入型网络技术，系统内角色权限可配、职责分明，事前风控、冲正补账的交易可控安排，信息最小披露、授权使用、隐私有保障，数据只增不减难篡改、全程追溯历史可验的技术逻辑。区块链技术具有去中心化、匿名、可追溯、不可篡改的技术优势，可以极大满足商品市场关于信任、隐私、效率的迫切需求。区块链采用分布式记账方式，信息分布存储在各个计算机上，由网络中多个参与者集体进行校验和维护。区块链技术的去中心化使得区块链技术的应用程序得以自动执行，无需依赖第三方的参与，也无需依赖司法机关的保障实施，从而自主实现数据的储存和记录，同时非对称加密

⑮ 夏纪森、臧志宏：《论区块链应用的社会风险与法律治理》，载《新华文摘》2019 年第 11 期，第 140 页。

⑯ 汪青松：《区块链作为治理机制的优劣分析与法律挑战》，载《社会科学研究》2019 年第 4 期，第 69 页。

验证使得其不可篡改。区块链技术的上述技术特征催生新型社会结构，形成“人——技术——人”的关系模式。而区块链技术规则在这其中扮演着重要的技术规制作用。区块链技术规则隶属于网络行为规范体系，它在技术层面上约束区块链网络的有关主体，就开发和利用区块链而制定技术要求和准则，使得区块链各构成部件得以协同运行，执行系统监督和有效的管理。

区块链系统内部存在不同的种类，不同的链上特性决定了技术规制的不同应用场域。根据区块链技术规则，“以节点准入的开放程度为标准，区块链系统可以划分为公有链、私有链和联盟链”。[17] 其中，公有链开源程度最高，私有链读写权限仅对某些节点开放，而联盟链开源程度介于前两者之间，属于针对有限第三方的部分开源，只能受限读取数据。不同系统类型区块链的性能评判标准各不相同。对于公有链系统而言，性能评判的关键是视其能否高效达成分布式系统各节点的一致性。公有区块链节点越多，处理数据的效率越低，越无法满足高并发的业务处理需求。区块链分布式存储记录的目的是为了防止篡改交易的各种攻击，重点是在去中心化的构架下如何提高公有链的效率，这也构成了公有区块链性能好坏的重要标准。相比之下，联盟链采用的是部分去中心化的网络架构，代码并非完全开源。在数据安全性方面，联盟链隐私泄露风险比公有链低。但联盟链由于去中心化程度低，节点数量扩展性差，会导致对中心机构信任不足的问题。而私有链采用的是可信中心的网络架构和有限的节点规模，其系统内记账效率远高于公有链和联盟链。此外，私有链系统在隐私保护的数据共享方面也具有独特优势。区块链技术上述不同链上特性决定了我们在面对不同区块链系统时需要采取不同的技术规制路径。

三、区块链技术应用风险规制的法治原则

对区块链技术的规制，既要积极鼓励和扶持网络信息技术的发展，推动创新驱动型经济的平稳发展，也需要避免让技术创造的网络新疆域成为脱法之地。这就需要从法治层面明确对其规制的基本原则。

（一）激励原则

在对新技术的规范中确立激励原则是为了通过对主体的能动性和主动性的有效激发、鼓励和调动，促使其采取有利于维护网络生态安全的行动。在技术发展的初期阶段，为了促进信息技术的研发和推广，实现经济加速向以网络信息技术产业为重要内容的经济活动转变，国家对于区块链技术的规制宜秉持鼓励技术发展的原则。一方面，该原则在区块链新技术的成长初期秉持对新生事物的包容和开放态度，给予其来自法律规范中人文品格的包容性和激励性；另一方面，在开放型经济环境中，该原则要求迅速把握区块链技术研发推广的时机，政策法规能够及时有效地沟通区块链技术与新市场，把区块链技术逐步转化为生产力，激励企业积极发挥动态效率优势。科技立法应当鼓励已掌握区块链技术的企业蓬勃发展。在宏观方面，通过立法手段保障和促进企业进行区块链技术的开发、推广；在微观方面，通过制度性安排措施保障和鼓励企业进行科研投资和技术人员的智力开发。长久以来，我国传统风险规制模式是自上而下主导模式，突出国家公权力的强力干预，弱化企业或其他主体的参与，忽视规制对象主体性和能动性，缺乏人文关怀和激励。这无形之中在规制主体和规制对象之间人为制造了对抗氛围，极易导致政府规制失灵的局面。

⑰　参见中国信息通信研究院：《区块链白皮书（2018）》，第1页。

而激励规制原则可以有效弥补传统压制型规制中有关机构能力不足的现实缺陷。从法经济学的视角分析，权力运作的成本随着权力运作范围的扩大而扩大。为了防止国家权力运作的低下，有必要考虑引入激励原则，给予区块链技术参与者及研发者更多政策扶持，营造良好的制度氛围，提高权力运行资源的有效性，释放被规制对象的主体能动性。

（二）创新原则

鉴于区块链技术迥异于传统网络信息技术，对区块链技术进行法律规制应着眼于其自身特点和问题导向。法律规制既不能过于冒进而有损创新，也要谨防落入规制万能主义的窠臼。创新规制是与传统压制型规制相对的概念，它基于对新问题的瞄准，进行治理方式上的创新。它要求针对区块链技术进行科学合理的划分，根据区块链技术应用发展的实时动态做出调整和纠正。该原则植根于新技术的特点和问题，开展规制视角和方式上的适度转变和创新。传统政府主导的规制对于缓解市场信息的不对称、切实保障消费者权益做出了有益探索和努力。当前区块链技术下的参与主体在数量和角色定位出现了新变化，法律需跳出既往立法窠臼，从区块链主体被化约为节点和数据的现实出发，重新确定有关交易者的独立人格与法律主体地位，创新区块链参与主体有关权利义务的内容。对区块链智能合约的规制要积极探索传统基本权利的新意涵。在区块链技术探索初期，立法创新应更多关注网络信息消化能力的孱弱以及围绕基于算法导致的系统结构性缺陷问题。这意味着法治需要对算法的基本设计予以强制性规范。在算法治理方面，传统互联网时代针对技术应用给特定当事人造成损害的法律后果，采用事后压制型规制追责方式来追究刑事或民事侵权责任。由于创新原则聚焦的治理根源和对象不同，与之相匹配的制度回应也应有所差异。传统压制型规制强调规制信息的供给，而创新规制更突出规制信息的真实性和有效性。后者更加突出对区块链网络生态内节点的权利分配与制衡，引入区块链系统内责任分配的新思路，[18]创设针对算法的科学性制约。[19] 同时，创新原则也要求执法机构在充分权衡创新与风险关系的基础上，对数据竞争和算法行为进行谦抑、审慎和动态的跟踪规制，建立容错试错机制，确保数据驱动型创新。

（三）区别化原则

区别化规制是指针对不同类型的区块链系统或同一种类型但不同应用功能的领域，分别采取不同方式和不同程度的法律规制，即根据不同行业和不同领域的特点分别确定规制重点、难点及规制程度，以避免“一刀切”式的压制型思维，提高规制的效率和效果。传统互联网技术规制可以划分为结构层面规制、功能层面规制和意识层面规制三个层面。具体而言，结构层面的规制围绕域名管理、IP 地址的分配等展开；功能层面规制覆盖通信工具、娱乐工具等具体应用领域的规制，包括对垃圾邮件和隐私保护的规制措施等；意识层面规制突出对意识形态等领域的规制，它包括防止文化间恶意的网络渗透、蓄意针对别国的言论煽动等。从时间的纵深发展来看，这三个层面的规制分别对应着传统互联网技术发展的不同时期。上世纪 90 年代初期是互联技术发展起步阶段，结构层面的规制对互联网技术的后续发展起到了重要作用。进入 21 世纪以后，互联网功能层面规制逐渐构成了互联网时代的主要规制方向。此后，伴随着互联网技术在社会各层面的渗透，互

⑱ 参见汪青松：《区块链系统内部关系的性质界定与归责路径》，载《法学》2019 年第 5 期，第 130 页。

⑲ 参见张凌寒：《算法权力的兴起、异化及法律规制》，载《法商研究》2019 年第 4 期，第 70 页。

联网意识层面的规制逐渐发展成这一阶段的重点规制面向。故区块链技术也遵循类似的区别化原则，对区块链的规制从代码层、机制层、行为层等层面逐渐形成了区块链治理的公共政策框架。

四、法治视角下我国区块链技术规制回应的选择

网络空间的法治化不仅要求法律对技术保持基本的包容和尊重，把握数字变革的内生逻辑和发展规律，也需要对技术保持高度的警惕。通过技术外部的价值附加及制度安排，攻克因技术缺陷导致的道德失落和自治困难，以平衡技术规则的自治与法律规范的他治，从而实现二者的良性共生，最终构建起多元化均衡治理的格局。

（一）多方配合打造协同共治格局

针对区块链智能合约的安全漏洞问题，应当构建符合我国国情的“共享法律服务”的新模式，实现法治治理、科技治理和多元主体监管的共治格局。在尊重技术规则的基础上，针对区块链技术结构性漏洞应积极开展新型规制，采取多方配合、联动治理机制。首先，相关部门应该以立法的形式确立智能合约协商更新机制。法律应当承认智能合约作为新型合同的法律地位，确立配套实施的基本制度，例如引入协商制度以及免责例外制度等等。创设协商机制目的在于使有关区块链参与主体能够积极参与智能合约中的条款协商，降低漏洞发生的概率，也可减轻修复漏洞的成本。免责例外的发生一般有以下几种特殊情形：因区块链技术数据传输的匿名性引发的身份欺诈；因意外事件或不可抗力导致合同责任的法定免除等。其次，设置专门的智能合约审查机构，负责对运行在区块链系统上的智能合约进行监管审计。在智能合约正式推出之前，必须经过代码安全核查机制展开全面细致的审核，确保将智能合约的漏洞发生率降至最低，抵御区块链系统的安全性风险。这些漏洞在智能合约上线之前都应被仔细地逐一排查。经过合规性核查之后，智能合约审查机构颁发上线许可。同时，为了保障合约执行阶段的合规性，应建立紧急调节机制。该制度通过设置紧急停止或转移合约功能的硬性要求来应对突发的合约漏洞事件。再次，建立智能合约漏洞报告和奖励制度。根据《网络安全法》关于强化网络信息收集分析和通报的有关规定，[20]以及《规定》明确指出的“区块链信息服务提供者应当接受社会监督”，技术专家团队如发现智能合约存有漏洞，应当第一时间报告区块链信息服务的提供者或有关行业监管协会，经核实无误，可获得来自国家和有关企业或单位的相应奖励。区块链信息服务的提供者一旦接到有关部门下达的补漏指令，应当在合理时间内对区块链的漏洞采取及时修补等措施以消除隐患。项目方在区块链项目上线前必须经过有资质的安全公司审计安全风险并获得通过。

（二）强化创新规制和国际合作

针对区块链信息技术权利被滥用的风险，应强化创新规制和国际合作。首先，我们应在我国现有法律框架内化解区块链新技术产生的法律问题。我国现有法律制度要求有关主体不得实施和帮助实施信息网络犯罪活动，即便是网络中立的帮助行为，若与网络犯罪的伤害结果存在直接或间接因果关系，都构成帮助信息网络犯罪活动罪的正犯。如果行为人利用区块链技术从事圈钱、行骗、隐藏违法犯罪所得，或者利用虚拟货币开展网络传销以及其他违法犯

⑳ 《网络安全法》第51条规定：“国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作。”

罪活动，那么应该在已有法律框架内赋予法律规制的新内涵。其次，在关系到国家经济命脉和金融市场秩序的领域，规定实名制放开的例外情形。在传统互联网信息技术下，《网络安全法》规定网络用户必须实名制。把实名制延伸到区块链技术的特定领域，将有助于缓解网络主体的隐匿状态与真实身份查证不一致的困境，切实保障国家金融监管秩序。但在其他公共部门，区块链应用技术宜适度放开实名制要求。一方面，从区块链技术本身的特性分析，区块链技术的匿名性和去中心化可以实现安全、高效、自由与透明的信息传递。这有利于充分扩大市场调节下的经济内需，激发市场活力。另一方面，在有限许可的领域放松实名制要求，以宽严相济的方式实现新技术与既有法制的有效衔接，可以为发展新型信息技术提供平台，形成鼓励创新的制度氛围。再次，在国际合作层面，应当加强各国在区块链立案标准和共同打击区块链犯罪这两方面的国际司法合作，构建起健康有序的区块链国际协同共治平台。该平台的创建有利于在全球范围内制定统一的《区块链协议指南》，强化区块链相关领域的国际协同共治，为最终建立国际化、开放型的区块链产业利益共同体提供条件。

（三）采取技术性应对策略助力法律实施

面对区块链系统内部的算法安全问题，可以通过技术能力的提升对抗区块链系统内部风险，为法律规制区块链算法风险提供技术保障。首先，区块链技术变革了权利界定的方式，使得法律关系的建构前提发生了本质改变，实现了权利界定的权威中心向分布式去中心的方式转变。传统的权利界定采取的是中心化一体式规制方式，主要包括财产权的国家信用保障，不动产物权登记，知识产权、股权的权属和变更登记等。只有基于传统上对权利合法性的认定，市场参与者才能就相关事实达成确信和共识。而区块链系统的权利界定是内在的和分布式的，通过去中心化的公共界定方式确保数据的真实、可靠与安全。该技术为权利的界定提供了全新的视角和途径。其次，区块链技术可以轻松解决当前著作权保护的注册、确权和验证等法律问题，有利于明晰知识产权法律关系中的权利义务关系。在著作权保护方面，数字版权管理系统和技术保护措施有效限制用户对数字内容的使用。区块链密码学技术使得著作权人在把作品写入区块链系统时，系统自动启用私钥进行数字签名。特定的第三方可以通过著作权人的公钥来验证数字签名的真伪。再次，针对来自区块链技术外部的量子计算威胁，通过量子安全加密和量子互联网技术，可增强区块链在法律事实认定上的有效性和科学性，完善法律归责体系。最后，提升区块链中数据传输的高效性和安全性确保区块链系统安全性。区块链内部关系结构的提升，为该技术助推法律服务奠定了扎实可靠的硬件基础；创新数字货币隐私保护安排，提高了用户隐私权保护力度和技术方法的规范性。对区块链技术的规制要求我们在技术的功能定位上改变单纯被规制的从属地位，实现技术辅助和强化治理的多重角色转向。

（四）实现区块链技术的价值形塑

区块链技术总体发展趋势如果脱离法律基本价值的束缚，则极有可能导致其对法律基本价值的破坏。法律的基本价值包括自由、平等、正义、秩序、安全等内容。它们植根于人作为社会主体的基本需要。如果区块链技术的发展与法律基本价值发生冲突，直接受害者便是作为社会主体的人。届时，人的自由权、平等权、生存权等基本权利便会因为区块链技术的存在和垄断而受到侵犯。倘若对区块链技术的负面影响不加约束，法律基本价值便会沦为区块链技术的牺牲品。被异化的区块链技术还会破坏法

律业已确认的基本伦理和道德规范。区块链技术给法律带来的首要任务是法律主体的再定义，明确法律主体的基本权利和义务。这要求我们建立起抑制区块链技术的负效应的法律理论体系和对策。为了保证区块链技术与法律基本价值的一体化发展，需要明晰技术研发的法律边界。具体而言，包括严格禁止特定研究内容、通过法律调整禁止成果侵犯公民基本人权、对区块链科研单位和科研设施设置必要的限度等。当然，在形塑区块链技术的价值架构的同时，也需要进一步调适既有法律知识结构，在充分了解区块链技术的基础上，根据实际需要适当地进行法律结构和内容上的调整，主动积极顺应时代潮流并通过及时补充区块链技术的科技附加值，逐步改善法律运行的环境生态。通过将区块链技术与法律基本价值进行深度交融，推动法律与区块链技术的有机融合，发挥法律在当代区块链信息社会中的统一调整职能。

Between Rules and Technology: Risk Analysis and Legal Regulation of Block Chain Technology Application

Jin Lu

Abstract: As the core driving force of the era of intelligent Internet, blockchain has brought great changes to human production and life style, but there are also technical regulation shortcomings and legal regulation difficulties. The violation of block chain technology application is mainly reflected in the realistic paradox of the security and efficiency improvement of consensus algorithm, the vulnerability risk of intelligent contract, the abuse risk of information technology rights and the value limitation of technical applications. It is an important institutional rehearsal for us to comprehensively meet the challenges of the era of "code law" and "digital governance", and it is of practical and urgent significance to discuss legal regulation of blockchain technology. The regulation of application risk of block chain should adhere to the principles of incentive regulation, innovation regulation and differentiated regulation. For the governance of the vulnerability risk of intelligent contract, we should adopt the innovative regulation method to create the pattern of multi - party cooperation and co - governance. To prevent the abuse of rights, we should not only curb the escalation of traditional problems, but also strengthen the rules for new problems. As to the resolution of algorithmic risk, it depends on technical strategy and makes technology helping law enforcement. Besides, it is also important to adjust legal mechanism to suppress negative effects of the technology thus help shaping values of block chain technology.

Keywords: blockchain technology; technical application risk; legal regulation

（责任编辑：李　辉）