区块链技术的监管风险与应对路径

左泽东,蒋先福

(湖南师范大学 法学院,湖南 长沙 410081)

摘要:目前,区块链技术在许多领域得到了广泛应用,但在多行业应用过程中存在着一系列风险,给监管机构的工作带来了很大的挑战。一是因体制缺陷而产生的"静态风险",具体表现为:法律实体与监管技术的缺失与滞后,现有法律与制度规范的适用难度大,技术标准与法律责任承担主体不明,分布式共享导致监管形态呈分散性,运动式执法与"一刀切"式禁令不合理等;二是因技术缺陷而产生的"动态风险",具体表现为区块链技术的自身漏洞与区块链技术的外部攻击。针对这两方面的风险,文章从政策与法律视角出发提出应对路径,旨在推动区块链技术营商环境、区块链技术监管立法以及实现区块链技术风险处理的法治化。

关键词:区块链技术;监管;静态风险;动态风险;法治化;应对路径

[**中图分类号**]D90 [**文献标识码**]A [**文章编号**]1672-934X(2020)06-0111-16

DOI:10.16573/j.cnki.1672-934x.2020.06.014

The Regulatory Risks and Respondent Paths of Blockchain Technology

ZUO Ze-dong, JIANG Xian-fu

(*School of Law, Hunan Normal University, Changsha, Hunan* 410081, *China*)

Abstract: At present, blockchain technology has been widely applied in many fields, but there are a series of risks in the process of multi-industrial applications, which brings great challenges to regulators. The first challenge is the "static risk" caused by institutional defects, which specifically includes the absence and lag of legal entities and regulatory technologies, the great difficulty in applying the existing laws and institutional norms, the unclearness of both the technical standards and the subject of legal responsibilities, the decentralized form of regulation caused by distributed sharing, and the irrationality of a removable type of law enforcement and one-size-fits-all prohibition, etc. The second challenge is the "dynamic risk" caused by technical defects, which specifically includes its own technical vulnerabilities and external attacks on blockchain technology. Basically, countermeasures from the perspective of policy and law have been proposed to promote the legalization of its business environment, supervision and legislation, and processing risk.

Key words: blockchain technology; regulation; static risk; dynamic risk; legalization; respondent path

一、引言

区块链的历史可以追溯到2008年10月31日,Satoshi Nakamoto发布了一篇文章——《比特币白皮书:一种点对点的电子现金系统》,这是一个重要的标志性节点。2009年1月,序列

收稿日期:2020-08-26

作者简介:左泽东(1994—),男,山西临汾人,硕士研究生,研究方向为现代法理学;
蒋先福(1956—),男,湖南桂阳人,教授,博士生导师,主要从事法理学、法制史等方面研究。

号是0的原始区块和序列号是1的区块相继诞生,两个区块形成的原始链便被称之为区块链。由此,区块链被正式推出。时至今日,区块链已发展十余年,其在金融领域、物联网和物流领域、公共服务领域、数字版权领域、保险领域、公益领域等均有所涉及,并推动了这些领域获得新的发展。更重要的是,《人民日报》曾作出报道,其将区块链视为新一代信息技术的代表之一,区块链技术的创新与互联网、物联网、大数据、云计算、人工智能、5G等并驾齐驱,表明国家对区块链技术的高度重视,也为区块链技术的未来发展注入了新的营养素。

2019年1月10日,国家互联网信息办公室发布《区块链信息服务管理规定》,旨在引导区块链应用向良性健康的态势发展。2019年10月24日,习近平总书记在中央政治局第十八次集体学习时重点强调,要加快推动区块链技术和产业创新发展,促使区块链迅速成为网络热词与研究热点,亦成为社会关注的焦点。此次强调意旨有二:一是作为核心技术的区块链在集成应用中起着重要作用,其将在新的技术革新中发挥独特的优势,为经济与科技发展助力;二是区块链技术在发展过程中并非一帆风顺,要规范和引导区块链良性发展,构建应对区块链安全风险的安保体系与安保机制,从严落实相关责任。因此,我们不仅要重视区块链技术的创新优势,还要重视区块链技术所引发的一系列风险问题,尤其是在众多适用领域的监管问题。

二、体制缺陷视角:区块链技术监管的"静态风险"

区块链,一个听上去具有神秘色彩的技术。"区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输与访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式方法。"[1] 区块链技术(Blockchain Technology,BT),是比特币的潜在或基础技术,也可将其称为"分布式账本或分布式数据库技术",其本质和精髓乃是一个"去中心化的分布式账本"。它的去中心化特征使其具有"分身术";它的匿名性特征使其实现"高效化";它的核心分布式记账功能使其具有"可靠性";它的智能合约功能使其具备"保护网"。但是,区块链技术的这些优势也容易带来很大的风险隐患,加大了监管机构的监管难度:去中心化的特征必将无限弱化中心系统的管理,使监管的成本与难度系数无限加大;匿名性特征使得责任主体不明确,加大查证、追踪、惩戒与监管难度;分布式记账的不可篡改性特征使得信息不可消错、过于固化、不可逆、失去灵活性,从而引发一系列法律风险;智能合约使其难以适应主观场景,致使主观与客观、技术代码与法理人情的分离,导致执行程序过于机械,缺失了情理空间;等等。具体表现在以下几个方面。

(一)法律实体与监管技术的缺失与滞后

目前由于我国尚未制定区块链技术规则的法律制度或技术标准,同时在区块链技术中缺乏中心化的法律实体,传统法律规则难以应用于分布式账本系统[2]。

第一,表现为法律实体的缺失与滞后。法律的稳定性必然导致其具有滞后性,而区块链技术在具体应用中产生的风险往往具有即时性与紧迫性,二者之间的矛盾与冲突进而将风险的处理推向泥沼:一方面,由于没有相应的法律制度做支撑、缺乏中心化的法律实体,致使风险的处理失去了"主心骨"。比如,就区块链技术的基础单位数据来说,其既非有体物、亦非无体物,《中华人民共和国民法典》(简称《民法典》)总则编第一百二十七条规定:"法律对数据、网络虚拟财产的保护有规定的,依照其规定";《中华人民共和国网络安全法》第七十六条第四项

规定："网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据"。两部法律规范皆对数据问题作出了规定，但对数据的归属权限、使用权限、责任承担与法律救济并未明确规定，倘若区块链中的数据发生泄露、窃取等风险，法律如何对其处理便成了"真空地带"。另一方面，由于立法程序的长期性与复杂性特征，常常导致风险问题的处理具有迟延性与不匹配性，出现法律与风险的"错位"。比如，"美国区块链科学研究所创始人 Melanie Swan 在其著作《区块链：新经济蓝图及导读》中将区块链分为三个阶段，即以数字货币为代表的区块链 1.0，以智能合约为代表的区块链 2.0，以及超越货币、经济、市场在司法、政府管理、公证等领域拓展应用的区块链 3.0。"[3]而这三个阶段的区块链风险问题的侧重点亦有差别，立法前与立法后面临的区块链发展阶段极有可能不同，而新阶段的区块链风险问题势必难以用旧阶段的法律规则来处理，从而使法律难以有效应对风险。

第二，表现为监管技术的缺失与滞后。与传统中心化监管的方式不同，区块链技术的去中心化特征使得中心无限弱化，其无限多的"分身"让监管机构难以应对。除此之外，如前文所述，区块链的每一个技术特征都无不加大了监管机构的监管难度，究其原因，这与监管技术的缺失与滞后紧密相关：首先，区块链技术使得监管机构难以采取检测、记录网络数据运行状态的措施，从而难以对风险进行检测评估，更无法建立检测预警制度与信息通报制度；其次，监管机构难以建立安全评估体系和应急工作机制、制定风险事件应急预案，很难判断风险事件的危害程度和影响范围，也很难对风险事件进行比较明确的分类与分级、制定相应合理有效的应急方案；再者，监管机构也无法采取有效措施介入区块链运行系统，难以防范区块链的外部侵扰与攻击、非法破坏与使用，难以保障区块链运行状态的稳定性、可靠性以及区块链数据信息的完备性、私密性与可使用性；最后，以目前的技术手段，监管机构难以探索或创制出一种凌驾于区块链技术之上的技术，从而对区块链技术进行"反制"，进而导致风险处理的紧迫性与技术手段的缺失性、滞后性之间的矛盾长期存在、难以消除。

（二）现有法律与制度规范的适用难度大

智能互联网时代的技术革命使现有法律制度面临着"破窗性挑战"和"创造性破坏"[4]。区块链技术在具体的应用中为各个领域创建了良好的客观环境与工作平台，极大提高了各个领域的运营效率，实现了价值的有效传递，同时也提高了信用难题。但是，区块链技术的迅猛发展态势与现有法律体系的固有稳定态势之间有着难以消解的长期矛盾，通常表现在智能合约的执行方面。与以"意思自治"为核心的传统合同有明显区别，"智能合约表现为交易方意志的运行系统，通过一系列的事先设计而得以执行，体现为合约与代码合二为一：合约由代码表示，同时由代码执行"[5]。亦即运用区块链技术成熟的加密算法程序来判断交易方的条件是否成熟，在条件未达到预设标准之前一直处于静默状态，一旦条件得到满足，合同或协议代码将会无意识、自动机械地执行合同或实施协议，实现合同或协议的履行。

然而，合约在自动执行过程中仍然有缺陷：首先，由于区块链技术具有不可篡改的特性，交易方的隐秘数据与私密信息一旦"上链"便不可逆，致使合同中交易方的"悔约权"丧失，相关法律与制度规范的适用便呈"空白"状态。其次，民法典合同编的内容与智能合约存有冲突，合同编的权利与义务、要约与承诺等规则是否亦适用于智能合约交易过程，或者说，随着区块链技术中智能合约的不断发展，其是否仍要像传统方式一样遵从《民法典》中合同编的相应规制呢？再次，智能合约的运营需要媒质，即完全凭

借计算机数字形式来载录数据信息并通过可计算的代码予以实施、执行,合同编的相关规则很难以技术代码精准体现,技术代码仅能体现规则的表面文字内容,但无法体现规则背后的法理意旨与制定意涵。最后,由于智能合约代码执行与传统合同执行方式不同,其机械性、单向性的特征使其缺乏灵活性,其敏捷性的特征使交易方很难有反悔的余地,这将使交易方的要约与承诺很难予以撤回或撤销,而建立于区块链技术之上的智能合约只能按照预设规则严格执行,致使具有灵活性的法律制度规范难以与不可逆的代码执行系统相匹配。总之,法律制度规范的适用难题将导致监管机构出现"监管断层"或者"监管破碎"现象。

(三)技术标准与法律责任承担主体不明

就像诚信原则是市场经济运行的根基一样,区块链技术亦是如此,也需要其运行根基。《2018年中国区块链产业白皮书》指出,区块链技术的许多特点都关系到整个金融行业的需求。因此,区块链技术已经应用到整个金融行业,并在其细分领域实现了大规模应用。随着区块链技术的不断创新、不断发展,其产业应用将越发成熟,延伸领域会越来越广,区块键技术"几乎在所有的产业场景都能落地应用,原因是几乎所有的产业场景都涉及交易,都有降成本、提效率、优化产业诚信环境的需求,而这正是区块链技术落地应用后能迅速发挥的作用"[6]。而区块链技术在诸多场景的落地应用中,必然离不开保障其良性运营的相应技术监管标准与行业技术规范。并且,由于区块链具有极强的技术难度与适用理解,"相应的监管部门对于区块链技术也缺乏明确的认识,监管标准和行业规范难以制定,也就导致了区块链技术应用的泛滥化"[7]。没有明确的技术监管标准与行业技术规范,使区块链技术应用泛化,进而同时导致监管的泛化。

此外,区块链的分布式记账技术实现了点对点的交易,摆脱了中介与第三方的中间区域,无需依赖中心化机构,使得私权自治更加盛行与彻底。在区块链技术下,每个区块中的参与节点都会实现匿名处理,并非使用自然人或法人的真实信息,具体表现为一连串的数字代码。换句话说,区块链是由全世界的匿名参与节点通过链接在一起的匿名计算系统来实现匿名交易的,并对账本予以分类。因此,在分类账本中根本没有各个节点参与者的真实信息,很难判断使用权人与所有权人是否一致,在实际交易中通常将二者等同。也就是说,在区块链交易中,基于对各个参与节点隐私的保密要求,交易方更侧重于关注交易的实质内容,至于对与其交易的参与者是否为本人可能缺乏关注或者根本不予关注。这就导致冒用、窃取他人身份信息进行交易或者杜撰虚假身份信息进行交易的现象大量涌现,使得具体的责任承担主体难以明确。不法分子正是通过利用身份信息与交易内容的弱相关性特征来实施不法行为,导致参与者身份的溯源极其困难,监管机构难以查证、追踪交易的具体信息流程,从而使不法分子顺利实现逃避监管的目的。更重要的是,如果这种区域性的不法行为蔓延至全国甚至全球,将极大增加监管难度,甚至会导致监管发生异化的风险态势。

(四)分布式共享导致监管形态呈分散性

"区块链是一个分布式的共享数据库。在分布式网络结构中,没有中央服务器,节点可以通过多条路径来互相通信。同时由于没有中心化的参与者,网络节点本身也是难以直接管控的。所以,从法律和监管意义上讲,节点设立的一般性规则仍不明确。"[8]因而,按照区块链技术的准入机制或者区块链账本公开程度的不同,换句话说,就是针对区块链技术的不同类型会有不同的表现形态。首先,是针对私有链的情形。"所谓私有链,是指系统的写入权限与读取权限是否对外开放、开放程度如何以及受到

何种程度的限制均受到某一组织或机构控制的区块链。”[9] 所以，私有链具有一定程度的封闭性与自治性。由于私有链的参与记账节点少且都是内部的节点，其本质仍由一个主体予以管控，与当下法律体系及监管体制兼容。其次，是针对联盟链的情形。“联盟链是指其共识过程受到预选节点控制的区块链，只针对特定某个群体的成员和有限的第三方，内部指定多个预选的节点为记账人，每个区块的生成由所有的预选节点共同决定。”[9] 联盟链的账本公开具有一定的程度化标准，即其介于公有链和私有链之间。并且，和私有链一样，联盟链也具有相对封闭的特性，且联盟链的各个参与节点具有相对独立性。最重要的是，私有链与联盟链节点的加入均需受到一定程度的控制与限制，简言之，就是要得到授权许可，因此二者亦可称为许可链，其一般都会预先设置一定的准入与中心管理机制，有比较明确的管控主体对上链的数据信息进行处理。

相对于私有链与联盟链，最具重大影响力的是针对公有链的情形。“公有链对世界上所有人开放，用户不需要注册和授权就能够匿名访问网络和区块，参与记账和交易，并且可以自由加入和退出网络。任何人都可以参与共识过程——决定添加何种区块到链上并确定其内容。”[9] 与私有链与联盟链不同，公有链是完全公开透明的，且不受任何主体控制或限制，任何人皆可参与，参与节点也完全平等。故而公有链也可称为非许可链。但是，在这样完全陌生且匿名的环境下，由于全球的任何主体均可介入，从而导致比特币、以太坊、EOS 等公有链项目的风险频发，致使公有链几乎完全处于没有明确的责任承担主体的状态。并且，由于公有链运用的广泛性，参与者平时接触到的大多数都是公有链项目，且公有链没有一个中心化的管控主体对其进行监管，不受任何机构控制，所以监管机构对公有链上参与节点的监管难度可想而知，其对公有链的监管呈现为一种分散性的形态。正如某些学者所说的那样，“传统金融机构具有‘固态形式’，比如通过看得见、摸得着的银行大楼，以此向客户展示雄厚实力和信用；而创新型科技支撑下的金融业则多具有‘液态化’特征，比如支付移动化，货币数字化和电子化，均仰赖‘液态’般的数据或信息在网络中高速流动。”[10] 近年来，依赖区块链技术的诸多行业呈“气态化”趋势发展，突破了域界限制，如空气般四处窜流，使得监管更为分散。

（五）运动式执法与“一刀切”式禁令不合理

针对区块链技术的监管，传统的以行政规范性文件进行规范监管的方式使得监管呈现从空白到全禁的极端形态：前期监管完全缺位，后期监管则完全禁止，一前一后两个极端。“这种不具备可预测性、完全依凭行政命令的运动式监管显然不利于金融科技创新与消费者保护，即便对于规制主体的全力以赴防范与化解重大金融风险的价值追求的实现亦明显不利。”[11] 并且，这些行政规范性文件的出台与风险的阶段性爆发紧密相关，具有临时性、随意性与依赖性特征，监管机构缺乏事先的谨慎通盘考量，一直都是小修小补、亦步亦趋，缺乏顶层设计的思量与探索，特别是在区块链技术应用密集的金融领域，这种现象格外突出，并且长期存在。这从侧面反映了一个客观的事实，即正如有学者所言：“运动式执法的持续存在，说明我们从来没有从总体上思考过金融市场、金融体制需要一个什么样的金融法律制度。”[12] 这种简单粗暴的、极易产生负面效应的运动式执法策略使得监管失去合理性，因而亟需建立一种持续性、完整性、有效性的常态化长效监管机制。

同时，监管呈现“一刀切”，这种禁令明显缺乏合理性。在 2013 年 11 月底，由于比特币价幅呈骤然走低的负向态势，引起了监管高层的高度关注。同年 12 月 5 日，由中国人民银行等五部门联合印发的《关于防范比特币风险的通

知》,对比特币的货币属性从法律地位上予以彻底否定,并对金融机构、支付机构的参与业务予以特别禁止,沉重打击了比特币市场,致其价格下跌30%以上。此后,相关参与机构迅速放弃比特币业务,各商业银行也对比特币交易与转账进行严格审查,由此,2014年的比特币市场变得严重萧条。在2017年发布的《关于防范代币发行融资风险的公告》(简称"九四公告")中,对首次币发行(ICO)活动予以全禁,严重影响了代币发行等一系列融资活动。结果,中国所有的加密货币交易所都被关闭,严重妨碍了区块链技术的发展。近年来,有些监管机构将虚拟货币或ICO与区块链等同,对区块链行业同样采取"一刀切"式的禁令,导致"一管就死"现象的出现,影响了区块链技术的创新,使得机构监管与技术创新之间的平衡问题难以调和,因而产生监管机构对区块链行业风险的忧虑与政府鼓励区块链技术创新之间的矛盾。

三、技术缺陷视角:区块链技术监管的"动态风险"

目前,区块链的技术价值更多反映在具象化的应用领域,而这离不开区块链的技术优势。首先,在区块链中,每个区块都与其他区块紧密相关,尤其是与其相邻的上一个区块联系密切,因为每一个后续区块都囊括了与其相邻的上一个区块的所有数据信息,即上一个区块全部数据包的数据指纹(哈希值),计算当前区块的数据指纹时,同时包含了上一个区块的数据指纹,形成一种稳固的特殊链接关系,一旦任何某个区块数据产生变动,后续所有区块的数据指纹都会随之发生变动,而变动了的数据会被所有参与节点发现、否认且丢弃,最终归于无效。在日常应用中,我们的区块链数据与所有节点同步。所有参与节点都知道区块的正确顺序,也可以查询相关数据,以保证区块链的防伪、防篡改和可追溯性。其次,区块链技术的去中心化记账方式,使每个节点都有一个账簿,所有节点都参与记账,使得账簿实时同步,变得公开透明,更加真实可靠;并且通过验证奖励机制,保证了记账节点不会作弊记假账,所有节点维护的同一账簿非常方便对账;而且,通过该算法,链上的所有区块及整个链的信息更加可靠。再次,区块链技术的三大记账规则:PoW、PoS和DPoS,直接关系到记账权和相关收益的分配,保证了记账的有效性,使共识机制成为区块链的灵魂。最后,区块链的匿名性可以在不泄露网络节点身份信息的情况下实现网络节点的正常交互,这依赖于非对称加密技术,且Merkle树、时间戳等技术可以保护数据的完整性。

总的来说,区块链价值与优势的展现是在区块链技术的数据层、网络层、共识层、激励层、合约层、应用层六个层级的技术架构基础上实现的。但是,区块链技术也并非完美无缺,仍然面临着自身技术的漏洞与外部技术攻击的风险,而这些隐患无不加大了监管机构的监管难度。上文提及的区块链技术面临着一些表层级的"静态"监管风险,这是区块链技术监管风险的基本原因。而区块链技术自身的漏洞与外部技术的攻击却是深层级的"动态"风险,无时无刻不在挑战监管机构的权威,这是区块链技术监管风险的根本成因。

(一)区块链技术的自身漏洞

区块链技术的广泛应用面临的最大风险是参与节点最需注意的"系统性风险"。所谓系统性风险,是指大多数区块链技术平台和应用所面临的价值风险,且这种风险是共同性的。换言之,不管是区块链货币、智能合约平台,乃至在此基础上衍生的应用,其价值皆会被这些风险所影响。系统性风险的发生或彻底解决,将对整个市场产生重大而深远的影响。

最重要的表现是区块链智能合约程序的安全性以及漏洞的特殊性和高风险性。区块链,尤其是部署在区块链上的智能合约,对程序的

安全性和脆弱性有着极其严格的要求，这是区块链和智能合约系统在短期内面临的最大风险。问题的关键是：谁在控制程序的部署和升级，这就需要了解链外程序和链上程序。对于链外程序，当发现威胁程序安全的漏洞时，程序可以快速升级，甚至根本不需要用户干预。最常见的是 Windows 的自动更新。链外程序之所以能做到这一点，是因为开发人员完全控制了程序版本的升级和部署。例如，针对 2017 年发生的 Linux SSL 漏洞，各大 Linux 发行商在第一时间做了补丁，随后全球系统迅速升级，在短时间内大规模解决问题。然而，区块链智能合约与普通的链下项目完全不同。一旦部署，程序发布者立即失去对程序核心逻辑的控制。因为区块链智能合约有“一经部署，不可更改”的特点，一旦出现程序漏洞或安全问题，我们只能眼睁睁看着程序被攻击、币被抢，没有办法紧急中止区块链项目。例如，在 2016 年的项目漏洞事件 DAO 攻击中，由于在众筹风险投资的 The DAO 合同代码中发现了漏洞，使得价值 6 000 万美元的以太币被盗。智能合约一旦部署，就不能修改。DAO 就是密码，密码就是法律。盗窃者是为了执行智能合约中一些隐藏的逻辑（漏洞）才能成功。无论是软分叉（区块链网络系统的升级和更新，升级前的节点都能很好地兼容升级后的节点，老节点继续接受新节点创建的区块，新节点和旧节点总是在同一条链上工作，并且没有生成新的链）后的 ETC 或硬分叉（升级前的节点不能与升级后的节点兼容，每个节点都延续自己认为是正确的链，原区块链将被分成几个独立的链，这可能导致新链的生成）后的 ETH，没有一个是可以补救的。程序的漏洞是无法避免的，只能尽可能优化，将风险发生的可能性降到最低。

Luu L 等学者将智能合约的漏洞分为交易顺序信赖漏洞、时间戳信赖漏洞、处理异常漏洞和可重入性漏洞[13]。王群等学者也有类似表述：交易依赖性（Transaction Ordering Dependence，TOD）漏洞、时间戳依赖（Timestamp Dependence）漏洞、可重入性弱点（Reentrancy Vulnerability）漏洞以及处理异常（Mishandled Exceptions）漏洞[14]。根据智能合约的脆弱性，Nikolic 等人将智能合约漏洞分为浪子合约、自杀合约、贪婪合约和遗嘱合约[15]。浪子合约是指智能合约执行后，通过智能合约的漏洞将交易资金转移到特定地址。自杀合约是指当以太坊发生故障时，契约的所有者有权选择退出，而当退出指令被其他节点执行的情形。贪婪合约是指当智能合约关联的商品和加密货币被锁定在以太坊时，交易双方既不能得到商品和加密货币，亦无法将合约予以取消的情形。遗嘱合约是指智能合约完成或关闭，代码和全局变量都已清除，智能合约仍能接收交易的情况。

此外，交易平台潜在的漏洞如控制台错误、用户账号安全、注册人和域名安全、网络协议安全等因素也会对交易平台及其用户产生负面影响。2018 年的利用漏洞赢头奖的 DEOS Games 游戏事件、Newdex 遭遇的 EOS 刷假币事件、日本的 Zaif 交易平台被盗事件、SpankChain 智能合约攻击事件以及遭遇两次攻击的 EOSBet 事件等，其主要原因就在于 EOS 的智能合约漏洞与交易平台漏洞的存在，导致损失金额非常高。

（二）区块链技术的外部攻击

一是表现为智能合约被攻击。在以太坊中，智能合约的交易过程会消耗 Gas，也就是以消耗以太坊费用为代价。若攻击者利用此特性对智能合约进行攻击，将会导致大量的以太坊费用被浪费。Teutsch 等人分析了两种可能的恶意脚本攻击：资源耗尽攻击和错误交易攻击[16]。另外，在智能合约中也存在 DDoS（分布式拒绝服务）攻击，也就是说，攻击者会将大量分散的、非集中性的恶意网络节点予以聚集，并利用这些聚集的恶意节点同时向智能合约系

统发起攻击,并进行反复操作,致使系统发生拥堵并消耗大量的以太坊费用。例如,“攻击者使用大量 extcodesize 操作攻击区块链系统。执行 extcodesize 操作时,Gas(以太坊成本)值非常低。攻击者在一个事务中可以执行 50 000 次此操作,从而大大降低了区块同步率”[17]。重要的是,攻击者可能利用犯罪智能合约获取机密信息、窃取密钥。比如,Juels 等人分析了一起使用犯罪智能合约窃取密钥的安全事件。攻击者利用犯罪智能合约 PwdTheft,结合 SGX(软件保护扩展)和 HTTPS(超文本传输协议安全性)等可信硬件技术窃取用户密钥[18]。

二是表现为黑客盗取数字资产。随着区块链技术的兴起和发展,大多数网络用户都会将一定比例的财富转化为数字货币资产,放到互联网上。此外,互联网是黑客的“大本营”,在这片“沃土”中,任何用户的数字资产都不可能绝对安全。更重要的是,大多数网络用户并不像黑客那样熟悉网络安全知识和操作系统。普通网络用户的这种关键能力缺陷使得黑客很容易窃取他们的数字资产。首先,与集中交易相比,黑客更喜欢分散交易平台。分散的交易平台,就像分散的钱包一样,自己的账户是自己管理的,所有权只属于自己。此外,任何人都不能篡改账户,也不存在无法取款的风险。然而,去中心化平台类似于匿名资产账户,谁持有密钥就会成为账户的所有者。当平台生成并交付页面的密钥以供显示时,持有者持有的就是唯一的密钥凭证。遗失、被盗、漏损等损失,一切责任均由持有者承担。然而,个人保管的密钥有时没有放在有严格安全措施的集中交换场所,这使得黑客更容易窃取个人的密钥。其次,黑客以各种方式窃取数字资产。比较常见的方式有:让木马劫持本地系统的主机文件,让木马修改本地网络配置 DNS 地址或路由器的 DNS,攻击相关网站的 DNS 缓存服务器,对运营商的 DNS 进行污染等,总之,黑客可以利用各种漏洞进行操作,比如做假的分散交易平台、假钱包、假网站等。此外,黑客窃取数字资产的方式主要是窃取私钥。例如,“梅耶尔在 ECDSA(椭圆曲线数字签名算法)方案中发现了一个缺陷。比特币和以太坊运行在一个特定的曲线上——secp256k1,而且,只生成私钥和公钥,这意味着所有参数都是公开的,信息可能会泄露。攻击者可以利用此漏洞复制用户的私钥。一旦用户的私钥被盗,很难恢复”[19]。施密特等人发现攻击者可以利用临时私钥攻击用户并窃取用户的签名私钥[20]。Courtois 等人提出了一类具有恶意随机数的攻击——ECDSA。如果两个用户在 ECDSA 方案中使用相同的随机数,则每个签名者都可以计算另一个签名者的私钥[21]。最后,黑客还可以通过攻击哈希函数来盗取数字资产。作为区块链技术加密算法的哈希函数,其仍然面临被攻击的风险。例如,Horalek 团队分析了利用彩虹表破解哈希函数,攻击者利用生成的彩虹表与哈希函数碰撞获取密码[22]。此外,哈希或散列长度扩展攻击(length expansion attack 是针对一些加密的散列函数的攻击,在消息和密钥的长度已知的情况下,允许额外的信息存在的攻击手法),也是攻击者破解哈希函数的一种方法[23]。

三是表现为 51%算力攻击。Satoshi Nakamoto 认为,“诚实节点的控制计算能力之和若大于具有合作关系的攻击者,则此系统是安全的。”也就是说,当具有合作关系的恶意节点的计算能力超过诚实节点控制的计算能力时,系统就有被攻击的危险。由控制 50%以上计算能力的恶意节点发起的攻击被称为 51%计算能力攻击。当然,并不是所有的加密货币系统都可能遭遇 51%的计算能力攻击。只有 PoW 共识机制符合条件,而非 PoW 共识机制则不可以。例如,以太坊有被 51%的计算能力攻击的风险,而 EOS 和 TRON 则没有。而遭遇 51%的计算能力攻击会有以下效果:首先,

体现在双花上。简而言之，“双花”是指一份“钱”已经花了两次甚至多次。例如，a 有 500btc，当 a 向 b 支付这些比特币时，a 也会将这些比特币发送到他的另一个钱包地址。也就是说，a 的一部分资金同时转移到两个节点。由于交易的时差，最后，发送给 b 的比特币交易被确认并打包成高度为 n 的区块，此时控制 50％以上计算能力的 a 发起 51％的计算能力攻击。a 重新组织区块 n 并将发送给自己的另一个交易打包到区块 n 中。此时，区块 n 包含两笔交易币。a 继续发挥其计算能力优势，在 n 区块上扩展，使其成为最长且合法的新链。这样，a 的 500btc 双花成功，b 钱包里的 500btc 就会“消失”。其次，一些地址可以被禁止发送或接收比特币。例如，a 和 b 之间存在矛盾，当 a 控制其 51％的计算能力并知道 b 的比特币地址时，就可能使与 b 有关的交易永远无法得到确认。假设 b 想把比特币发送到 Genesis 地址。利用计算能力的优势，a 可以让所有其他节点不打包此交易。如果其他节点挖出的新区块打包了本次交易，a 将选择在该区块之后不再继续延伸，而 a 将在新区块的上一个区块之后快速重建自己的新区块，从而阻断 b 的交易。依靠自身的计算能力，从 a 分支出来的链将成为最长的合法链。此时，其他节点必须放弃与 b 的交易，否则，与 b 进行交易的其他节点可能面临被孤立和失去回报的风险。然而，需要强调的是，即使拥有超过 50％的计算能力，也不可能颠覆系统共识。例如，不允许“偷币”，因为这个操作需要私钥签名。如果想伪造一个签名，诚实的节点便不能容忍这种行为，这将破坏系统共识。此时，其他诚实节点在被“偷币”节点挖出的区块后，不会继续扩张区块链，诚实节点会主动扩展合法区块，“偷币”节点挖出的区块将被隔离。另外，修改系统出块奖励的行为也不能执行。例如，将出块奖励从 10btc 改为 100btc 也颠覆了系统的共识。诚实的节点将拒绝非法区块并派生出一个新的链。最后，是自私的挖矿攻击。这种情况下，攻击者将挖掘出的区块连接到私有链上，私有链从区块链系统中分出，使该链比公链长，并阻止其他节点知晓。当私有链的长度太长而不能被公共链驱动时，攻击者会发布私有链让其他节点知道，从而获得主链的状态。诚实节点在不知情的情况下承认该链，并继续在该链上进行挖掘，从而使得诚实节点无法得到回报。

四是表现为“预言机”被攻击。一般来说，强大的区块链项目具有数据不可篡改（包括 51％的计算能力攻击）特点。更重要的是，这种不可篡改是指数据的真实性更重要，因为假数据即使不能篡改也没有价值。区块链应用程序通常需要从现实世界获取真实数据。这些数据在互联网上很容易获得，但是对于区块链应用，它需要某种方式和机制来调用。这种方法在区块链中被称为 Oracle，即预言机。它不同于在互联网上直接调用中央信息提供者（如房价信息）的数据接口。Oracle 的核心任务是以分散的方式访问这些真实数据，以确保这些数据不被篡改并安全地传输到区块链应用程序。通过多方投票产生一定结果是 Oracle 的常用方法之一，它适用于某些特定场景，如选举、重大事件等。在这种情况下，投票者受到利益的制约，即通过抵押代币的方式，但效率并不乐观。以 Oracle 的一个主要应用场景 DeFi 领域为例，其需要大量的高频数据交互和验证，因为此时 Oracle 需要一个更快、更可靠、更高效的数据采集和验证机制，包括使用更多的数据源，构建两层网络＋随机节点组获取数据。然而，对于金融服务业来说，如果数据出错，损失也是“高效率的”。例如，区块链资产平台 synthetix 在 2019 年 6 月遭遇 Oracle 攻击事件，当数据遭到攻击后，交易机器人立即发现问题，开始自动交易，造成短时间内高亏损。平台最终与交易机器人的主人取得联系，协商减少损失，也幸好是

因为交易机器人的使用范围相对较小,否则,被广泛使用且成功攻击的后果就难以想象。

五是表现为P2P网络被攻击。首先,攻击者会恶意造成网络的延迟或者对网络进行隔离,从而发动攻击,这主要表现在以下四个方面:包括Heilman E等人提出的日蚀攻击(即攻击者独占受害者的业务连接,并将受害者与系统中的其他节点隔离)[24];Gervais A等人提出的可伸缩度量攻击(即攻击者利用比特币的可伸缩性来延迟交易信息的传输)[25];Apostolaki M等人提出的BGP劫持攻击(即攻击者通过阻塞区块链的网络流量,进而实现延迟网络信息的有效传输或区块同步的速度)[26]以及Natoli C等人提出的余额攻击(指低计算能力攻击者暂时中断具有相同计算能力的子组之间的通信)[27])。其次,区块链技术并未做到完全匿名,仍有不足之处。P2P网络是连接区块链各个节点的主要媒介,并且,P2P网络中存在三种异常的中继模式,这已被Koshy等人确定,即攻击者可以对比特币地址加以利用,助其找到所对应用户的计算机网际协议地址[28]。个人信息也可能通过交易方的交易行为泄露,Androulaki等人,已经总结了六种交易行为,而这六种行为都有可能泄露个人信息。通过在大学进行比特币交易货币的实验,发现通过聚类分析的方法来解析交易行为,可以获得用户大约40%的个人数据[29]。攻击者也可能通过女巫攻击(即利用单个节点,并利用该节点伪造多个身份,这样便可以对系统进行攻击,达到破坏系统的冗余机制的目的)[30],从而达到将分散的匿名协议予以破坏或阻止的目的,致使交易方真实身份泄露。此外,除了交易方的真实身份信息外,交易方的交易隐私也面临被窃取的风险。比如,弗莱德等人,提出攻击者可以将两种力量予以结合,一个是外部信息资源,另一个是信息流分析技术,利用两种合力优势来分析典型的用户行为、消费和查询习惯,以及同一用户多个账户之间的比特币流量,这样,用户的交易隐私便被窃取[31]。

(三)"动态风险"的监管反思

针对区块链技术的自身风险和外部攻击,很多学者提出了不同的对策。比如,针对私钥安全问题,Gennaro提出了一种基于ECDSA的门限签名算法来保护比特币钱包;Pérez-Solà等人提出了一种利用特殊的比特币脚本FR-P2PK来预防双花攻击的交易机制;针对智能合约,Luu L等人提出的一种智能合约漏洞分析器Oyente以及Zhang F等人提出的Town Crier;针对区块链隐私的保护技术的点对点混合协议、环签名、非交互式零知识证明以及Hawk框架技术;等等[32]。并且,还有一些学者也提出了应对观点,比如,直接应对机制、引入异构的区块链系统[33]。虽然这些学者提出的应对措施有效缓解了区块链技术的自身漏洞与外部攻击问题,但是在实际应用中仍然有很高的技术难度与成本开销。此外,这些学者的观点有的仍处在理论模型的探索阶段,还未进行仿真实验,缺少实验数据与模拟支撑,因而没有足够的说服力。构建一个干净的、良好的区块链环境平台,完善严格的区块链审查机制或许是应对区块链技术监管的最有效措施与最主要的趋势。

四、区块链技术监管风险的应对路径

无论是区块链技术表层级的"静态"风险,还是区块链技术深层级的"动态"风险,都考验着监管机构的监管能力。一方面,如何保证区块链技术的创新发展;另一方面,如何处理与应对区块链技术产生的风险。二者之间如何有效地平衡始终是监管机构面临的最大难题。其实,自2013年开始,我国政府便对区块链活动予以监管,逐渐形成了初步的政策立场与法律框架。在政策立场方面表现为:对分布式账本的积极认可、对数字代币的严厉监管、对智能合

约的谨慎观望、对区块链平台服务的有力支持。在法律框架方面表现为：引导区块链发展的法律框架（包括各地进步条例、奖励办法、民企规定；各地信息化条例、地方性法规、地方政府规章、政府数据管理办法；食品安全与大气污染领域关于数据或信息平台的法规）与预防区块链风险方面的法律框架（包括预防网络风险、金融风险与犯罪风险的法规）[34]。但即便如此，区块链技术的创新发展与风险监管之间的张力并未消弭，二者之间的平衡点仍需监管机构努力探寻。

（一）法律层面的应对路径

一是积极探寻立法，缓解适用矛盾。目前，区块链技术正呈极速发展的良好势头，技术的系统更新与升级较快，但专门针对区块链技术进行科学、民主、依法立法的条件与时机尚未成熟。此前，已出台一部关于区块链技术的高位阶立法——《密码法》。此部法律的实施对区块链技术的规制功不可没，但是，也只是解决了区块链技术的一部分规制难题。基于科技视角，区块链是一种涵盖数学、密码学和计算机编程等多个学科的技术。基于该体系的结构模型，区块链系统由数据、网络、共识、激励、合约和应用六个技术层面组成。基于核心技术，区块链主要包括分布式账本技术、非对称加密技术、共识机制、智能合约等。因此，区块链技术的立法应遵循由点到面、分类攻克、重点突出、详略适度的原则。首先，要从可编程货币、可编程金融、可编程社会三个方面着手，探索应用层立法；从脚本代码、算法机制、智能合约入手，探寻合约层立法；从发行机制与分配机制入手，探索激励层立法；从 POW、POS、DPOS 等机制着手，探索共识层立法；从 P2P 网络、传播机制与验证机制入手，探寻网络层立法；从数据区块、链式结构、哈希函数、非对称加密、时间戳、Merkle 树等入手，探索数据层立法，从而实现从点到面、分类攻克的原则。其次，对区块链的核心技术领域进行重点式、微观式的立法，对区块链的非核心技术领域进行全面式、宏观式的立法，实现核心技术领域风险的有效规制、非核心技术领域风险的有效预防，实现重点突出、详略适度的原则。最后，立法工作人员应积极与区块链技术所涉及的众多学科的专业人员进行合作，使法律与技术学科互融，实现立法的精准性与适当性，从而完成监管的顶层设计。

此外，可利用网络技术对风险高发的区块链技术领域与应用领域进行科学预警与通盘考量，提前做好规范措施，出台应急立法预案，避免制定法律规范时长期存续且具有负面效应的随意性、临时性与依赖性。一方面，有助于解决法律制度规范的缺位与滞后难题，缓解区块链技术因发生风险面临的无法可用、用法冲突等适用法律的难题。另一方面，也有助于解决行政规范性文件长期以来小修小补的困境以及监管机构的运动式执法模式，从而有利于推动一种持续、完整、有效的常态化监管机制的建立。

二是代码法律互补，技法理性融合。法律的价值更多在于指引和预防，从而使得行为人的行为合法与预防纠纷的发生。而代码则是区块链技术的执行媒介与运行基础，所以，技术规则可通过代码这个媒介对风险予以事先预防。法律与代码均有其自身的缺陷：一方面，法律规范的模糊性使其容易产生歧义，容易导致法律规范的不确定性，降低执行效率；另一方面，代码执行的机械性与单向性特征使得代码失去了灵活性，变得固化死板。而区块链和法律同为信任机制，若二者之间关系不确定，区块链技术便难以良性发展。它们应该是相辅相成、优势互补的关系。正如凯文·沃巴赫所言，“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。”[35]一方面，“法律代码化”可以将法律规范的具体内容、意旨融入代码，借助代码技术，

使法律执行更具敏捷性与确定性;另一方面,“代码法律化”使得代码汲取法律规范的情理法理念,以及自治、法治与德治协同治理的模式,使得代码执行更具有灵活性。

此外,区块链技术与法律的融合应遵从理性融合的理念,即二者之间的融合必须有主有辅。换句话说,二者之间的融合并不意味着二者的规范效力处于平等性地位,相反,二者之间应以法律规范为主、以技术代码规范为辅,并保证主从有序。并且,从自治、法治与德治三方协同治理的视角予以考量,此三者之间亦处于非平等关系的状态,也是有主有辅,因而,应将代码技术规范纳入自治范畴,使其符合法律规范的要求,确保代码技术规范的运行始终处于法律规范的指引与监督之下。这样,不仅从形式上实现了二者的互动,而且从内容上实现了二者的调适,从而形成技法融合、多元规范协同治理的区块链系统,最终解决法律规范与技术代码规范之间的适用冲突,消除二者之间的隔阂,并避免“监管断层”与“监管破碎”的现象。

(二)政策层面的应对路径

一是实施分类监管,确保主从协调。分类监管指的是针对区块链技术应用的具体领域,从而发挥各个领域监管机构的优势作用,实现对区块链技术的分类监管。一方面,可以进行微观监管,比如,金融方面的区块链应用由金融监管机构来监管,法律方面的区块链应用由司法机关来监管等。另一方面,也可以进行宏观监管,比如,国家层级的各个金融行会、各个网络协会联合起来对区块链进行国家层面的监管。在金融监管方面,国外如英国、美国、新加坡等都采用了“沙箱监管”模式。简言之,“监管沙箱就是一块试验田,监管者为之提供真实的市场环境。虽然不进行干预但一直予以监控,如果能够排除系统性风险方能允许市场普及,否则予以清退,由此实现了监管与创新的平衡。”[36]其精神在于,通过对区块链金融的限制性监管来激励金融创新、防范系统风险。例如,在“供应链金融、证券保险行业的广泛应用领域引入监管沙盒,监管沙盒有助于监管者在创新中发挥建设性作用,通过监管措施的主动调整,促进市场创新的主动实现,将被动响应、等待风险事件驱动的监管理念转变成为主动引导的理念”[37]。在法律监管层面,我国借鉴国外“沙箱监管”的理念,实施有针对性和更灵活的软法治理模式,避免了“一刀切”的做法。这种引入“沙箱监管”的分类监管模式不仅大大提高了监管效能、降低了系统风险,而且也为相关规定的制定与实施提供了借鉴。

除此之外,自律调节这种自我监管方式应该被大大鼓励与强化,以便实现《区块链信息服务管理规定》第四条的宗旨。除了法律监管这股主力外,相应的行业自律制度、行业准则以及行业自律协会应予以大力协从,一主一辅、相互协配,共同助推区块链的良性监管。正如美国学者凯伦·杨所言,“区块链之所以能够吸引无数拥趸,在于其能够规避传统法律的程序负担和交易费用,实现高效可靠的人际社会合作。”[38]故此,更应让自律调节发挥其独特优势,让监管更具有弹性。一方面,这可强化政府与行业间的沟通,让政府更加了解区块链技术的行业应用现状,确保监管的及时性与有效性;另一方面,自律调节可以让行业监管机构更理性地看待与应用区块链技术,也可以让新兴行业的管理更加合理,从而推动区块链应用行业有效健康发展。

二是注重人才培养,加强国际合作。要解决区块链技术的监管风险,不仅要重视技术开发,更要加强对专业人员的培育与储备。首先,要加强区块链相关行业专业人才的培育和储备。目前,区块链技术在各个行业的应用非常广泛,呈现出规模化的趋势。因此,区块链技术在相关行业应用的技术标准尤为重要。就拿近年来诸多行业推出的产品溯源问题来言,如果

没有这方面的专业人才，就无法对区块链技术在此模块的运营有一个清晰明确的认识，也就无法建立一套完整、合理、有效的行业评估体系与行业准入制度，容易导致此行业违法犯罪的风险。因而，需要在区块链应用成熟的行业领域加强专业人员的培养，并积极借鉴国际上区块链技术应用较为成熟的行业技术标准，只有对行业有了充分了解，并具备了充足的专业人才，才可以构建更好的监管模式。其次，要加强区块链技术人才的培育与储备。一方面，针对区块链技术的自身系统漏洞，根据分布式账本技术、非对称加密技术、共识机制、智能合约等区块链的核心技术进行有针对性地重点培养。还需加大对该核心技术的研究力度，体现实时性、前瞻性与合法性、合理性，且区块链技术的数据、网络、共识、激励、合约、应用六个层级以及每个层级包含的各个模块均需进行前沿研究，将区块链的核心技术、六个层级以及其所囊括的各个模块的基础知识与前沿研究一并传授，使学员具备完整性、实时性的知识架构。另一方面，对于区块链技术的外部攻击，需要进行技术上的“反控”。在对区块链技术进行系统细化研究基础上，加强专业人员对“反区块链技术”的探究，其主要目的在于增强区块链技术的自身防御能力，反制区块链技术的外部攻击并强化自身监管，形成以“新链”治“旧链”的“以链治链”模式。

另外，区块链技术具有“去中心化”的特征以及突破界域限制的性能，因此，对区块链技术监管也必须突破界域限制，形成监管合力。正如有学者所言，“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。”[39]而该平台的创建，可以凝聚各个国家的监管力量，在全球范围内搭建一张监管网络，使得监管不再分散，也有利于制定全球化的、统一性的区块链应用与监管规范，从而强化国际协同共治。并且，在详细分析全球区块链技术的监管政策后，我们可以看到：“美国区块链监管政策步步为营、欧洲各国区块链监管思路清晰、亚洲各国区块链监管两极分化”[40]。虽然各个国家均有关于区块链技术的监管政策，但是取得的成效却有差异，监管力量仍然分散于各个国家或各个大洲，监管效果也是强弱分明、参差不齐。为此，须打破国域与洲域限制，使各个国家间互联互通，彼此吸收区块链监管政策的优点，在国际上成立“区块链应用与监管联盟”，遵循“互联互帮”的原则，从而建立起一种系统——基于国际化、透明化、开放性、民主性的区块链监管网络系统。

（三）法律与政策结合应对

一是在“链外”加强审核，严格法律门槛。加强链外审核，即在用户上链之前，应严格限制准入条件，加强对用户的资质审查，并对用户的真实身份进行严格的准入审核和登记。比如，上海市《互联网金融从业机构区块链技术应用自律规则》第八条规定：“互联网金融从业机构应当加强客户身份识别、认证，严格遵循实名交易、‘了解你的客户’等原则，并加强平台之间的互联互通；严格遵循反洗钱相关规定，对可疑交易及时发现、及时上报”。第九条规定：“互联网金融从业机构应该积极贯彻落实国家网络安全战略，全方位关注区块链技术的设备安全、数据安全、系统安全、秘钥安全，及身份证认证机制、权限管理系统。”不难看出，这两条自律规定均对上链用户的身份认证做了明确规定，意在确保其身份信息的真实性与可靠性。虽然区块链技术的上链用户在区块链平台上是完全匿名的，在交易中也可用密钥代表其身份，但并不意味着用户的真实身份信息可以忽略。相反，对于上链用户的真实身份信息不容忽视，更应严格把关：一方面，可以严格规范用户的交易行为，降低用户利用区块链的“匿名性”特征进行违法犯罪行为，并有利于出现违反犯罪行为之

后责任主体的确定;另一方面,对用户身份的认证和对可疑交易的及时发现与上报的义务也可以规范区块链平台对自身的监管,一定程度上保证区块链技术的设备、数据、系统与密钥的安全,降低区块链平台的风险发生率,减少监管机构的监管成本。

二是在"链内"注重联合,凸显政策导向。在"链内"应当特别注重区块链与人工智能的联合。2018年12月2日,《人民日报》就曾报道:"人工智能和区块链是密切关联的两种技术,两者可能会在未来日益融合,共同推动智慧社会发展。"而基于互联网、大数据、算法的人工智能技术,其在自动规划、智能搜索、自动程序设计、智能控制、指纹识别、人脸识别、机器人学等方面的实际应用恰好可以弥补区块链技术不精确和不确定的管理。首先,人工智能技术的指纹与人脸识别可以大大提高链外审核的效率,并大大提高追踪与确定责任主体的效率。其次,人工智能技术的智能控制优势可以对风险进行预警并检测评估,建立检测预警制度与信息通报制度,并对风险进行分级化与分类化处理,建立严格的安全评估体系和合理的应急工作机制,制定相应有效的风险事件应急预案。再者,人工智能的自动规划与自动设计程序可以对区块链技术的自身漏洞做出合理化的智能弥补,有效防范区块链的外部侵扰与攻击、非法破坏与使用,保障区块链运行状态的稳固性、可靠性以及区块链数据信息的完备性、私密性、有效性与可使用性。最后,人工智能技术与区块链技术一样,可以突破界域限制,利用其优势可以对区块链应用行业进行"去中心化"的智能监管,以便扭转区块链行业一直呈"气态化"的分散监管窘境。

五、结语

本文基于区块链技术发展过程和行业应用中的一系列监管风险,将区块链技术的监管风险分为静态与动态两类风险,并对其进行了较为深入的分析。最后,针对区块链技术的两类风险,提出了一些相应的且较为合理的应对路径。而对这些风险的分析与具体应对路径的探索主要有三大要旨:一是要实现营商环境的法治化目标。营商环境涉及市场主体的政务、市场、法治、人文环境等有关影响市场主体活动的政治、经济、社会、法律等一系列外部因素和条件。这样可以从制度层级为营商环境的持续优化提供保障与支撑。二是要实现监管立法的法治化目标。这不仅可以使加强引导行业自律调节、试点现行,使行业内部规则成熟运行,进而以点带面,逐步推进,实现科学立法的目标;而且可以使监管主体在制定规则时不会独断专行,充分鼓励市场主体积极参与,广集民智,实现民主立法目标;更重要的是,可以促使监管主体在规则制定前对区块链产业与风险予以全面考量,依照立法程序,推动国家层级的相关立法,实现依法立法目标。三是要实现风险处理的法治化目标。这可以推动监管机构制定合理的风险处理程序,确保监管与执法主体处理风险的合法化;还可以保证风险处理过程中的公平、公正、公开,并实时接受社会监督;可以保证当监管与执法主体出现的违反风险处理程序、违反法治的普遍性与一致性要求时,对其予以严格追责、严格惩戒。最终目的是确保监管机构的监管有一个制度化防御体系。

不难看出,区块链技术在发展过程中或具体行业的应用中或多或少总会出现一些新型的风险,而这些风险势必会给监管机构的监管带来难度,挑战着监管机构的权威。鉴于此,有学者提出:"针对区块链领域存在的风险及其对监管的挑战,应从法治角度给予规范和治理,让法治成为提升区块链技术竞争力的基础。"[41]推进区块链技术朝法治化方向发展确为应对其风险监管的最佳路径。当然,有效平衡区块链技术的风险监管和技术创新也是必要的。一方

面，“在社会治理和公共服务中，区块链有广泛的应用空间，将有力推动社会治理数字化、智能化、精细化、法治化水平”[42]；另一方面，对区块链技术的风险予以有效监管同样不可忽视，在“区块链行业发生风险之后，应严格依据法治的普遍性和一致性要求进行处置”，“在行业的风险处置方面，应该严格参照法制规定的程序处理，避免走极端化路线”[43]。二者务必同时兼顾，不可或缺。目前，在区块链技术的“动态风险”方面仍有诸多技术漏洞与新型攻击方式尚未被发现，解决这些问题的关键仍需区块链技术不断更新、不断升级以及培养相应技术人才。至此，区块链技术已历经三个阶段，希望在区块链技术发展的下一个阶段，这些风险问题可以得到有效解决。

[参考文献]

[1] 何波. 区块链技术及其法律问题[J]. 中国电业，2018(5)：56-59.

[2] 吴悦舒. 区块链的行业应用及法律风险分析[J]. 学术争鸣，2019(4)：57-66.

[3] [美]梅兰妮·斯万. 区块链：新经济蓝图及导读[M]. 龚鸣，等，译. 北京：新星出版社，2016：1-2.

[4] 马长山. 智能互联网时代的法律变革[J]. 法学研究，2018(4)：20-38.

[5] 王延川. 智能合约的构造与风险防治[J]. 法学杂志，2019(2)：43-51.

[6] 孙占利. 链式反应：区块链的法治意义与功能[J]. 法治论坛，2020(54)：289-305.

[7] 赵磊，石佳. 依法治链：区块链的技术应用与法律监管[J]. 法律适用，2020(3)：33-49.

[8] 和涛. 区块链监管需要新思路[N]. 人民邮电，2020-06-30.

[9] 赵磊. 区块链类型化的法理解读与规制思路[J]. 法商研究，2020(4)：46-58.

[10] 黄震，邓建鹏. 论道互联网金融[M]. 北京：机械工业出版社，2014：25.

[11] 朱娟. 我国区块链金融的法律规制——基于智慧监管的视角[J]. 法学，2018(11)：129-138.

[12] 彭冰. 反思互联网金融监管[J]. 金融博览，2018(12)：36-37.

[13] Luu L，Chu D H，Olickel H，et al. Making Smart Contracts Smarter[C]. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM，2016：254-269.

[14] 王群，李馥娟，王振力，等. 区块链原理及关键技术[J]. 计算机科学与探索，2020(7)：1-24.

[15] Nikoli C I，Kolluri A ，Serger I ，et al. Finding the Greedy，Prodigal，and Suicidal Contracts at Scale[C]. Proceedings of the 34th Annual Computer Security Applications Conference. ACM，2018：653-663.

[16] Luu L，Teutsch J，KulkrniR，et al. Demystifying Incentives in the Consensus Computer[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM，2015：706-719.

[17] Jeffrey Wilcke. The Ethereum Network is Currently Undergoing A DOS Attack[EB/OL]. (2016-09-22). [2020-07-18]. https://blog. ethereum. org/2016/09/22/ethereum－network－currently－undergoing－dos－attack/.

[18] Juels A，Kosba A，Shi E. The Ring of Gyges：Investigating the Future of Criminal Smart Contracts. //Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM，2016：283-295.

[19] Mayer H. ECDSA Security in Bitcoin and Ethereum：A Research Survey[J]. Coin Faabrik，2016(28)：124-129.

[20] Schmidt J M，Medwed M. A Fault Attack on ECDSA[C]. 2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). IEEE，2009：93-99.

[21] Courtois N T，Valsorda F，Emirdag P. Private Key Recovery Combination Attacks：On Extreme Fragility of Popular Bitcoin Key Management，Wallet and Cold Storage Solutions in Presence of Poor RNG Events[R]. Cryptology ePrint Archive：Report 2014：848.

[22] Horalek J，Holik F，Horak O，et al. Analysis of the Use of Rainbow Tables to Breakhash[J]. Journal of Intelligent & Fuzzy Systems，2017(32)：1523-1534.

[23] Coron J S，Dodis Y，Malinaud C，et al. Merkle-Damgrd Revisited：How to Construct a Hash Function[C]. Annual International Cryptology Conference. Springer，Berlin，Heidelberg，2005：430-448.

[24] Heilman E，Kendler A，Zohar A，et al. Eclipse Attacks

on Bitcoin's Peer-to-Peer Network[J]. IACR Cryptology ePrint Archive,2015:129-144.

[25] Gervais A,Ritzdorf H,Karame G O,et al. Tampering with the Delivery of Blocks and Transactions in Bitcoin[C]. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM,2015:692-705.

[26] Apostolaki M,Zohar A,Vanbever L. Hijacking bitcoin:Routing Attacks on Cryptocurrencies[C]. 2017 IEEE Symposium on Security and Privacy (SP). IEEE,2017:375-392.

[27] Natoli C,Gramoli V. The Balance Attack or Why Forkable Blockchains are Ill-Suited for Consortium[C]. 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE,2017:579-590.

[28] Koshy P,Koshy D,Mcdaniel P. An Analysis of Anonymity in Bitcoin Using P2P Network Traffic[C]. International Conference on Financial Cryptography and Data Security. Springer,Berlin,Heidelberg,2014:469-485.

[29] Androulaki E,Karame G O,Roeschlin M,et al. Evaluating User Privacy in Bitcoin[C]. International Conference on Financial Cryptography and Data Security. Berlin,Heidelberg: Springer,2013:34-51.

[30] Douceur J R. The Sybil Attack[C]. International Workshop on Peer-to-Peer Systems. Berlin,Heidelberg: Springer,2002:251-260.

[31] Fleder M,Kester M S,Pillai S. Bitcoin Transaction Graph Analysis[J]. arXiv,2015(6):1-8.

[32] 张杰.区块链安全综述[J].西安文理学院学报(自然科学版),2020(3):37-47.

[33] 斯雪明,徐蜜雪,苑超.区块链安全研究综述[J].密码学报,2018(5):458-469.

[34] 苏宇.区块链治理的政府责任[J].法商研究,2020(4):59-72.

[35] [美]凯文·沃巴赫.信任,但需要验证:论区块链为何需要法律[J].林少伟,译.东方法学,2018(4):83-115.

[36] 崔志伟.区块链金融:创新、风险及其法律规制[J].东方法学,2019(3):87-98.

[37] 邓建鹏.美国区块链监管机制及启示[J].中国经济学报,2019(1):125-130.

[38] [美]凯伦·杨.区块链监管:"法律"与"自律"之争[J].林少伟,译.东方法学,2019(3):121-136.

[39] 金璐.规则与技术之间:区块链技术应用风险研判与法律规制[J].法学杂志,2020(7):84-93.

[40] 刘宗媛,黄忠义,孟雪.中外区块链监管政策对比分析[J].网络安全空间,2020(6):19-24.

[41] 邓建鹏.区块链法治化监管需要大智慧[J].人民论坛,2020(2):112-115.

[42] 巩富文.以区块链赋能社会治理[N].人民日报,2019-11-21.

[43] 邓建鹏.区块链监管的法治进路[J].衡阳师范学院学报,2020(1):27-35.