

# 区块链去中心化的法律治理研究

翟新丽, 于 寒

(郑州大学法学院, 河南 郑州 450000)

**摘 要:**区块链技术作为一种新兴技术,在给众多领域带来新机遇的同时,也引发了一系列法律风险。为实现技术应用与法律规制的深度融合,有效应对新技术对现有法律规制的冲击,对区块链去中心化所引发的司法管辖不明确、责任追究困难、数据泄露风险等问题进行研究。针对研究结论提出以下对策:推动协作式监管,完善司法管辖争议解决机制;精细化管理用户身份,建立责任认定机制;技术创新与法律规制协同保障数据安全,提升抵御风险的能力。旨在使区块链去中心化所引发的法律问题在一定程度上得到解决,促进区块链合法合规发展。

**关键词:**区块链;去中心化;法律风险;监管

**中图分类号:**D922

**文献标识码:**A

**文章编号:**1673-131X(2022)01-0023-06

区块链自出现以来一直备受关注,目前已经上升为国家战略,被确定为新基础设施。区块链是一种将数据区块按时间先后顺序进行排列组合而形成的链条式数据系统<sup>[1]</sup>。区块链技术是继大数据、云计算之后又一项颠覆性新兴技术。纵观区块链技术应用实践可以发现,这一技术在一定程度上解决了人们长期存在的信任危机问题,但是没有中心化的管理机构也就缺少对数据信息安全进行保护和承担法律责任的中心主体。2021年,去中心化金融(DeFi)平台上黑客盗窃活动猖獗,利用虚拟货币诈骗的案件资金标的高达100多亿美元,全球范围内约有70亿加密货币被盗。这类案件的发生使未来区块链技术应用面临严峻的安全形势。

区块链最核心的特征——去中心化,是区块链区别于其他数据系统的最主要的特征。去中心化使节点之间的信任成本十分低<sup>[2]</sup>,但去中心化与系统安全之间存在一定程度的矛盾冲突。由于目前区块链相关立法依据缺乏,立法理念保守,司法方式单一,相关程序性规则、技术性操作规范还不完善,因此只有从去中心化这一核心特征出发,找出该特征束缚区块链技术发展的内外因,才能有针对性地对其进行法律层面上的完善。此外,区块链去中心化还引发了人们思维方式的变化,需要我们从

法律治理层面去审视区块链技术给经济和社会发展带来的挑战,从法律价值层面反思这项技术所改变的思维方式以及适用的方法论等问题。鉴于此,本文以区块链去中心化的法律治理问题为研究对象,分析去中心化所引发的法律问题,并反思相关法律监管方式,研究并提出相关法律治理措施,以期实现法律保障效果的整体化和最大化,助推国家治理体系和治理能力的现代化<sup>[3]</sup>。

## 一、文献综述

目前,学界对区块链的研究大多集中在统计学、密码学、计算机技术等领域。从法学角度对区块链相关法律问题进行的研究主要涉及以下两个方面:

一是区块链技术应用领域的法律风险研究。在金融领域,曹玉昆等认为区块链技术的应用给金融监管主体的界定、金融机构法律责任的明确、金融违法行为的法律规制等方面带来了法律风险,需搭建智能化科技监管平台,构建多元业务监管制度,以推动金融监管方式转型<sup>[4]</sup>。在数字版权领域,石丹指出区块链去中心化简化了授权许可程序、完善了权属证明机制,为版权许可制度提供了

收稿日期:2022-01-25

基金项目:中国法学会2020年度部级法学研究课题“黄河流域生态保护司法保障制度研究”(CLS2020ZZ034)

作者简介:翟新丽(1979-),女,河南郑州人,讲师,博士,主要从事环境与资源保护法学研究。

新的建设路径,并重点研究了区块链技术在版权许可和保护领域的应用问题<sup>[5]</sup>。在个人信息保护方面,王从光通过对区块链运用到个人信息保护领域的内在法理逻辑进行分析,试图建立技术与法律双向融合的二元治理结构,以摆脱传统法律治理的窠臼<sup>[6]</sup>。区块链被犯罪分子利用,成为犯罪工具,进而所引发的刑事风险也是学者们较为关注的问题。张庆立研究了区块链技术应用中犯罪行为的具体表现以及刑法认定标准,并在程序法上予以回应,以确保妥善处理区块链刑事案件<sup>[7]</sup>。此外,还有不少研究集中在智能合约的法律性质和法律效力方面,如焦经川从肯定说和否定说两个方面对智能合约是否属于法律合同进行分析,并试图利用“监管沙箱”理论建立一种科学的监管方式<sup>[8]</sup>。

二是区块链法律监管层面的研究。凯伦·杨等分析了传统法律规范与区块链内部规制间的交互关系,并以此为基础考证区块链法律监管与自律监管的利弊,提出了一种全新的治理模式<sup>[9]</sup>。赵磊等则在借鉴美国和日本监管模式的基础上,提出应对区块链技术的应用进行类型化管理,加强产学研三方面的交流,以提高治理效能和风险防控的能力<sup>[10]</sup>。总体来说,目前学界从法律层面展开的研究呈“碎片化”状态,研究角度和内容的前瞻性与创新性不够。另外,纵观区块链技术发展趋势,未来区块链势必会与云计算、人工智能等数字技术相结合,这必将加大对其所引发的法律问题进行规制的难度。

随着区块链技术的不断发展,学者们对区块链去中心化特征日益关注。李伟重点分析了去中心化在司法区块链中的管辖问题与执行问题,提出构建以法院为主导的争议解决机制,更好地优化司法资源配置<sup>[11]</sup>。王延川检视了去中心化所引发的法律风险和利益冲突,创新性地提出了新中心化和再中心化的应对之策<sup>[12]</sup>。

通过对上述研究成果进行分析可以发现,目前还比较缺乏以区块链技术自身特点为切入点展开的研究,但正是区块链自身特点使其成为一项备受关注的先进技术,而其应用潜能还未被完全开发就已经引发了一系列法律问题,阻碍了区块链技术的发展。区块链去中心化研究的广度和深度仍有待拓展,有效的法律治理是区块链有序发展的保障。

## 二、区块链去中心化所引发的法律问题

### (一)跨境交易监管不明,司法管辖难以确定

传统的跨境交易都有银行作为中间机构进行统一监管,因为银行具有较为完善的管理体系,可以有效地对交易行为进行监管。在区块链技术支持下的资产跨境转移,如跨境交易、跨境支付等,则不需要第三方机构即可完成。虽然这在一定程度上提高了跨境交易的效率,但区块链去中心化也颠覆了传统的金融交易规则,冲击了现行的监管制度。如果某项交易行为在境外合法,而在国内却违反了相关法律,那么利用区块链技术向我国境内公民提供服务,是否应当以违反了我国的法律而被追究法律责任?在跨境交易监管不明的情况下,一些犯罪分子在区块链平台上层层操作转手洗钱的违法犯罪活动也日益猖獗<sup>[13]</sup>。这些问题亟待解决。

区块链中每个节点的用户都是匿名的,在被告身份无法确定时,没有专门的中心机构为节点的运作承担法律上的责任,也没有中心机构对节点进行监管,无疑是对传统地域管辖的一大挑战。在出现涉及我国和他国的区块链纠纷案件时,可能会出现案件侵权行为地和合同履行地分别在我国和他国的情况,由此就会产生不同乃至冲突的司法管辖,在适用法律过程中,如何利用现有《民事诉讼法》和相关司法解释确定司法管辖或实现法院排他性管辖也是一大难题。此外,一些不法分子利用比特币等虚拟货币在区块链平台上进行涉嫌欺诈的ICO(initial coin offering,首次币发行)融资、恶意逃税等非法活动,而在惩治犯罪分子时由于地址不明,身份无法确定,经常出现法院之间相互推诿的现象,案件审理难以开展。可见,区块链平台上跨境交易的司法管辖权有待进一步明确。

### (二)用户匿名化,责任追究困难

匿名化可以理解成去中心化的衍生特征。区块链各节点之间没有信任机制,也无法识别对方身份信息,只通过节点地址和共识机制进行信息交换,即使获取了节点上完整的区块信息,也无法知晓用户的真实身份,由此引发责任追究困难问题。

以智能合约为例,匿名化的特点可能会使合约当事方以匿名的方式或者虚假的身份出现。这虽然有利于保护当事方的个人隐私,但是也存在隐患。一方面,匿名当事方的民事行为能力难以辨别,在某

些情况下可能导致合同无效或可撤销等情况发生;另一方面,当合约当事方没有输入正确代码,导致其真实意思无法准确表示,造成损害或产生争议时,受害方难以通过诉讼等方式获得救济<sup>[14]</sup>。即使可以通过缺席判决进行裁决,但也可能由于当事方匿名化特征,致使判决后的执行程序根本无法进行,判决成为一纸空文。

再以比特币为例,美国多个执法部门曾联合查获一个从事非法入侵系统、提供虚假身份信息办理证件、买卖违禁药物等活动的电子平台。该平台将比特币等虚拟数字货币作为支付工具,平台上的参与者也都匿名,执法部门因此很难追寻到在平台上从事违法犯罪活动的嫌疑人,进而难以追究其法律责任。

目前,我国在《网络安全法》中明确规定,网络运营者在进行网络操作和提供网络服务时,应当要求用户提供真实身份信息。此外,国家互联网信息办公室发布的《区块链信息服务管理规定》也要求落实真实身份信息认证制度。若不进行身份信息认证,平台将不为该用户提供服务。这也就意味着,从某种角度来说,未来区块链平台的用户将不具备匿名性。但是,在国际上很多国家并没有相关规定,对于我国公民在以太坊等国外平台上进行交易后出现纠纷时,该如何应对匿名化所带来的相关问题,是我们需要解决的难题。区块链中每个节点的用户都是非实名的,参与交易的各方主要通过节点地址来获取信息。这就为金融诈骗、勒索钱财、洗钱等违法活动提供了便利,增加了犯罪的概率。虽然《区块链信息服务管理规定》的实施在一定程度上制约了匿名化的犯罪行为,但是目前在不法分子隐藏身份信息进行违法犯罪活动时,仍缺少侦查和处置的专项规定。

### (三)数据不可篡改,权利难以救济

数据不可篡改主要是指存储在区块链上的数据不可篡改和不可删除两个方面。第一,所有参与者在区块链网络节点上操作的信息经过系统处理上传至区块链网络之后,仅从某个节点对数据进行修改是无意义的,独立的操作行为不会使系统中的数据产生任何变化。第二,删除权是指用户发现之前存储的信息有错误时,享有合法删除的权限。在出现某种情况时,网络用户在符合条件的情况下有权利要求网络运营商删除相关数据,但是在区块链网络中则无法删除。区块链上的操作几乎是无法改变的,数据一旦被区块链所记录则很难篡改。如果要修改已经被区块链所记录的信息,数据的变更成本极大,除

非能够同时控制系统中超过51%的节点,否则数据将会永久存储在系统中,不再发生变动。但是同时控制整个系统中超过51%的节点的代价极高,涉及多个主体、多方面的利益,几乎很难实现。

在用户个人层面,信息公开在使网络用户享受信息交流和共享所带来的便利的同时,也给数据保护带来了潜在风险。在区块链网络中,用户个人信息和任一环节的任一操作都会被记录在区块链平台上,只有同时正确使用公钥和私钥,才可以访问数据信息。但是如此严密的算法并不代表用户数据的绝对保密。只要掌握了公钥和私钥,其操作规则和数据内容就等同于公开的,在毫无信任的基础上数据便可以进行交流。

在现代网络技术背景下,经常有用户需要修正数据的情况发生,例如,忘记密码需要重新设置密码、被盗的账户需要找回等。如上所述,只有同时正确使用公钥和私钥,才可以访问区块链数据信息,私钥由用户个人自行保管,一旦丢失,用户将无法对账户进行修改或找回,任何人或机构也无法获悉区块链中存储的信息,更无法证明其权属,缺乏相应的救济机制。但如果不法分子利用技术手段破译了私钥,那么就等于将用户的账户信息一览无余地展示出来,不法分子可以随意操作这个账户。如果发生此类情况,权利被侵害了,如何找到侵权人?损失怎么弥补?如何救济?从另一个角度来看,在用户的信息被泄露后,由于区块链数据的不可篡改性,一旦数据信息被公开,那么将对用户的个人隐私及财产信息构成永久的潜在风险。

在平台服务商层面,区块链平台作为第三方机构,具有为用户提供技术支持和平台服务的职能。在平台用户信息被泄露的情形下,平台服务商为避免公信力丧失,就需要负担巨额的赔偿金,平台因此损失惨重<sup>[15]</sup>。以区块链平台为代表的新型信息泄露问题不断出现,传统的数据监管已经无法满足当下数据安全保护的需要,不适应区块链行业的发展趋势。这也是区块链去中心化在数据信息安全方面所面临的一大难题。

## 三、区块链去中心化的治理之策

区块链去中心化所引发的法律问题已经阻碍了区块链产业的健康发展。当前,区块链技术已然成为一项核心技术,它带来的范式性影响也愈发明

显。对于这项技术,如果只是盲目地鼓励和促进,不进行规制和监管,那么势必会给市场和经济发展带来较大的法律风险。因此,在科学分析的基础上如何规范区块链技术的应用,如何应对区块链去中心化所带来的一系列法律问题,已经成为当前区块链发展中不容忽视的重大课题。相关部门应对去中心化所引发的法律风险进行有效防范,更好地推动区块链行业健康有序发展,促进区块链技术升级,使之成为利国利民的技术。

### (一)推动协作式监管,完善司法管辖争议解决机制

1. 推动法律监管方式转型,实现协作式监管。区块链技术本身具有复杂性、多层性和叠加性等特征,具体表现为区块链技术的应用往往跨行业、跨地区、跨部门。这就导致了不同的应用可能由不同机构监管或多个机构共同监管。为了节约监管成本、提高监管效率,可以采取跨部门协作监管方式进行监管。例如,在金融交易过程中,在缺少中心化管理机构的情形下,出现向境外转移逃税所获得的非法收入时,就要同时受到财政税收管理机构的监管和央行对跨境交易业务的监管<sup>[16]</sup>。在这种情况下,就需要法律明确跨境交易的监管组织和监管范围,细化监管权限,推动监管协作,打击利用区块链技术转移非法所得的行为,保障合法跨境交易业务的正常运行。需要指出的是,各个国家关于跨境交易的法律规定各不相同,可能会在交易过程中出现各种争议,因此在跨境交易出现问题时,解决争议的办法也需要法律进行明确规定。协作式监管方式能弥补单一监管机构在专业能力上的不足,拓宽监管渠道,使监管的手段和策略更加灵活,有助于降低系统性风险,较好地应对区块链给公权力的公信力带来的挑战。

基于上述分析,对区块链应用的协作式监管可以从以下三方面着手:一是建立数据共享平台,加强监管部门之间的信息交流;二是加强监管部门之间的合作,构建部门间协作机制和风险防范机制,形成和谐的合作环境;三是建立区块链应用风险评估、预警及应急机制,减少市场交易侵权行为和犯罪行为的发生。

2. 建立适应区块链去中心化特征的管辖规则。区块链去中心化引发争议的重要原因之一就是司法管辖不明确。虽然没有中心管理机构承担法律责任,但并不代表其虚拟地址背后参与主体的法律责任可以豁免。因此,首先应明确链上司法管辖,

增加“数据操作影响地”作为司法机关在被告身份难以确定时的特殊管辖地。其次,借鉴传统的属人、属地原则来解决在司法管辖问题上所遇到的难题。在区块链司法管辖问题上,可以类推适用一般侵权案件的管辖规则,同时参考网络侵权案件的管辖规则,也可以对区块链虚拟节点进行物化,以确认其所在地。进一步来说,可以以虚拟财产实际控制地为依据来确定管辖问题。这样既解决了当事人寻找虚拟财产所在地的困惑,也避免了在虚拟财产所在地不明的情况下,法院间相互推诿或恶性诉讼竞争的出现<sup>[17]</sup>。最后,可在区块链技术应用地区设立区块链专门法院或法庭,对区块链相关案件进行集中处理,降低管辖重叠所带来的法律风险。此外,要对区块链案件进行分类管理,统一各类案件的审判标准,避免地方保护主义和部门主义影响司法公正。

### (二)精细化管理用户身份,建立责任认定机制

1. 完善顶层设计框架思路。首先,加强区块链规范化发展的法律保障。虽然国家出台了一系列法律法规,为区块链的发展提供法律保障,但现行法律法规还存在一些与区块链技术应用相冲突的地方。针对区块链去中心化所引发的相关问题,应出台专门的法律法规、司法解释和区块链应用的精细化管理规定,并通过发布典型指导案例等形式,明确链上权利属性、数字货币法律性质、智能合约法律界定及法律效力等问题,弥补区块链技术应用的法律空白,为区块链应用监管的执行提供法律依据<sup>[18]</sup>。其次,加强对用户身份的管理。根据平台不同开放程度,采取不同监管策略,进行不同程度立法,即秉持开放程度与立法强度正相关的原则,从公有链到私有链,监管力度应由强到弱,涉及范围应由宽到窄,立法强度也应由强到弱。最后,应以全局整体的视角审视去中心化所带来的法律风险,结合具体应用场景,建构以国家立法机关为主体,以政府、企业、平台和其他参与者为共同参与者的多元化主体,对用户身份进行精细化管理,促进区块链应用更快地落地实施。

2. 建立区块链相关案件责任认定机制。去中心化衍生的匿名化导致了责任追究较难。这很大程度上是由区块链自身技术特点以及区块链专业性和技术性较强所引发的。由于缺乏同时具有区块链技术知识和法律知识的审判人员,因此法官在责任认定时存在一定的困难。因此,应借鉴我国现行知识产权审判中的技术调查官制度<sup>[19]</sup>,对负有

责任认定职责的主体进行统筹的制度安排,建立区块链相关案件责任认定机制,解决举证责任分配问题,将技术人员作为专家辅助人引入区块链相关案件责任认定中并参与审判。加强技术侵权案件审判队伍建设,精准查明案件事实,优化区块链纠纷司法诉讼解决机制。

司法机关应运用大数据、人工智能等技术对区块链相关案件的责任承担进行预评估,提高审判效率。要在法律系统内建立起强大的安全防线,加强对个人信息和链上数据信息的保护,分析现行区块链相关法律法规的可行性与实践性,探讨解决区块链纠纷的合理途径和案件事实的认定机制,以保障区块链的可持续发展。

### (三)技术创新与法律规制协同保障数据安全,提升抵御风险能力

1. 技术创新与风险规避并行,区块链应用与法律治理同频共振。立足当下区块链发展趋势,加快底层技术的原始创新。加大研发投入,突破原有思维定式,提升区块链自身风险应对能力,同时,在法律层面把握好技术创新与法律规制之间的关系,最大限度地发挥区块链技术的功能优势。

在国家层面上,要出台有关用户隐私保护及配套的平台救济专项法规,其中应包括保护用户个人隐私安全、建立权利受损救济途径、明确平台服务商赔偿标准等方面;在地方层面上,在不违反宪法和其他法律法规的前提下,制定与地方行业特色相符合的区块链专项政策,增强法规的灵活性和可操作性,推动政策与法律之间的有效衔接<sup>[20]</sup>。同时,将法律条款代码化,以实现实时监管。具体而言,将法律条款以代码形式写入区块链中,从而对链上数据及其交易进行实时监管。例如,在智能合约中,可将与合约内容、数据安全、保密条款等相关的法律法规写入区块链中,从而在合约履行过程中通过法律代码化来审查合约的履行情况是否符合法律规定。监管人员还可以与技术人员合作,将相关领域的法律规范转化成依据代码运行的规则,通过区块链运行程序和算法来实现监管的自动执行,减少监管成本,及时迅速地对出现的法律问题作出反应。

2. 建立平台资质认定和准入机制,完善权利救济途径。区块链平台服务商在发展初期可能存在主体不明确、资质不合格、技术不稳定等问题,因此应建立平台资质认定机制,统一资质认定尺度,制定准入标准,将“准入—经营—责任承担”全过程都

纳入法律监管。这有利于提升区块链平台的服务质量,提高抵御内外安全风险的能力,引导区块链技术更好地合法合规发展<sup>[17]</sup>。

在出现数据泄露等问题,权利需要救济时,需要赋予除区块链平台和参与人以外的第三方主体权利,对受害方予以救济,其中一个重要的主体就是区块链行业协会。行业协会应贯彻法律监管为主、行政监管为辅的理念,对行业内的行为进行规范,对违反行业规范的行为进行处置,对权利受损的主体予以救济。行业协会要根据《区块链信息服务管理规定》对区块链技术应用行业进行自律管理,坚决抵制行业内的违法犯罪行为。行业协会应积极履行主体职责,引导从业人员提升行业自律意识,推动行业信用评价体系建设,提升行业协会的治理效能,真正保障区块链行业利益相关人的权益,为区块链营造良好的发展空间。此外,可以将区块链行业内部管理制度转化为代码,通过代码化形成体系化的链上监督,提高行业内部管理治理能力,提高监管效率。实现技术治理与法律规制的协同监管,是未来区块链监管的重要方向之一。

## 四、结语

当下区块链正处于飞速发展的阶段,未来势必会带来一场新的产业变革。区块链去中心化就像一把双刃剑,一方面提升了经济社会的发展水平,另一方面也不可避免地会带来行业乱象。进入区块链3.0时代后,探索区块链健康发展的法律治理措施显得更加重要。现有区块链去中心化法律治理措施仍在实践中,虽然在法律监管层面已经取得了一些成绩,但是仍存在短板,去中心化的纠纷解决机制也没有很好地发挥效用。综合衡量区块链技术的利弊与风险防控的要求,针对区块链去中心化所引发的法律问题,应建立一种体系化、规范化的法律治理机制。在法律层面,既要完善顶层设计,又要坚持技术创新与法律规制同频共振;既要明确司法管辖问题,又要建立相关责任认定机制和平台准入机制,使之符合区块链技术应用内在机理。此外,还应重视法律人才与技术人才的培养,放眼国际,密切关注区块链各项应用的发展方向,深入研究区块链具体法律问题,为区块链健康发展创造良好的外部条件。

## 参考文献:

- [1] 何波. 区块链技术及其法律问题[J]. 中国电信业, 2018(5): 56-59
- [2] 陈蕾, 周艳秋. 区块链发展态势、安全风险防范与顶层制度设计[J]. 改革, 2020(6): 44-57
- [3] 张巧良, 王珍珍. 基于区块链的众筹融资风险管控策略探究[J]. 财会通讯, 2021(24): 121-123
- [4] 曹玉昆, 翟相如. 区块链金融的法律风险及监管路径[J]. 人民论坛, 2020(30): 120-121
- [5] 石丹. 论区块链技术对于数字版权治理的价值与风险[J]. 科技与出版, 2019(6): 111-120
- [6] 王从光. 区块链技术应用与个人信息保护的法理解读与治理[J]. 西北民族大学学报(哲学社会科学版), 2021(6): 107-117
- [7] 张庆立. 区块链应用的不法风险与刑事法应对[J]. 东方法学, 2019(3): 72-86
- [8] 焦经川. 区块链与法律的互动: 挑战、规制与融合[J]. 云南大学学报(社会科学版), 2020(3): 128-144
- [9] 凯伦·杨, 林少伟. 区块链监管: “法律”与“自律”之争[J]. 东方法学, 2019(3): 121-136
- [10] 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
- [11] 李伟. 司法区块链的“去中心化”困局与出路——以“去中心化”争议解决机制为研究对象[J]. 西南政法
- 大学学报, 2021(3): 87-99
- [12] 王延川. “除魅”区块链: 去中心化、新中心化与再中心化[J]. 西安交通大学学报(社会科学版), 2020(3): 38-45
- [13] 吴燕妮. 金融科技前沿应用的法律挑战与监管——区块链和监管科技的视角[J]. 大连理工大学学报(社会科学版), 2018(3): 78-86
- [14] 李佳伦. 区块链信任危机及其法律治理[J]. 法学评论, 2021(3): 118-129
- [15] 张茜, 金春阳. 国际贸易中区块链应用的场景与法律风险管控[J]. 长安大学学报(社会科学版), 2020(5): 20-28
- [16] 安文靖. 自贸区跨境贸易区块链应用的法律困境与对策[J]. 人民论坛, 2021(15): 85-87
- [17] 张生, 李妮. 区块链的“司法化”: 发展、挑战与应对[J]. 西安交通大学学报(社会科学版), 2021(1): 127-135
- [18] 杨锦帆. 基于区块链的纠纷解决机制研究[J]. 陕西师范大学学报(哲学社会科学版), 2021(4): 163-176
- [19] 陈存敬, 仪军. 知识产权审判中的技术事实查明机制研究[J]. 知识产权, 2018(1): 41-49
- [20] 陈立洋. 区块链研究的法学反思: 基于知识工程的视角[J]. 东方法学, 2018(3): 100-108

(责任编辑: 唐银辉)

## Research on the Legal Governance of the Decentralization of Blockchain Technology

ZHAI Xin-li, YU Han

(Zhengzhou University, Zhengzhou 450000, China)

**Abstract:** As an emerging technology, the blockchain technology not only brings new opportunities for many fields, but also causes a series of legal risks. In order to achieve the deep integration of technology application and legal regulation and to effectively deal with the impact of new technology on existing legal regulation, this paper studies the unclear jurisdiction, the difficulty of accountability, the risk of data leakage, and so on problems caused by the decentralization of blockchain. According to the research conclusions, the following countermeasures are put forward: promote collaborative supervision and perfect the resolution mechanism of jurisdictional disputes; refine the management of user identity and establish the mechanism of responsibility identification; technological innovation and legal regulation jointly ensure data security and improve the ability to resist risks. It aims to solve the legal problems caused by the decentralization of blockchain to a certain extent, and promote the legal and compliant development of the blockchain.

**Key words:** blockchain; decentralization; legal risks; supervise