Open Journal of Legal Science 法学, 2023, 11(1), 143-155
Published Online January 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.111021

Hans汉斯

区块链赋能知识产权保护：风险识别和规避

刘雪凤，张　笑，张文萱，郗文玉

中国矿业大学公共管理学院，江苏　徐州

收稿日期：2022年11月25日；录用日期：2022年12月6日；发布日期：2023年1月17日

摘　要

区块链的应用能促进知识产权保护的智能化、提高知识产权保护效率。已有文献聚焦于区块链赋能知识产权保护的技术特征以及不同应用场景，风险研究不足。论文识别区块链赋能知识产权保护中的法律风险、信息风险、监管风险和知识产权风险，并探讨风险产生的技术机理。作者提出：应该构建“法律规范 + 政策监控 + 技术自治”三位一体的风险规避机制，以提高知识产权保护效率。

关键词

区块链，知识产权保护，风险识别，风险规避

Blockchain Energizing Intellectual Property Right Protection: Risk Identification and Avoidance

Xuefeng Liu, Xiao Zhang, Wenxuan Zhang, Wenyu Xi

School of Public Management, China University of Mining and Technology, Xuzhou Jiangsu

Received: Nov. 25th, 2022; accepted: Dec. 6th, 2022; published: Jan. 17th, 2023

Abstract

The application of blockchain can promote the intellectualization of intellectual property protection and improve the efficiency of intellectual property protection. The existing literature focuses on the technical characteristics and different application scenarios of blockchain enabled intellectual property protection, and the risk research is insufficient. This paper identifies the legal risk, information risk, regulatory risk and intellectual property risk in blockchain enabled intellectual property protection, and discusses the technical mechanism of risk generation. The author

文章引用: 刘雪凤, 张笑, 张文萱, 郗文玉. 区块链赋能知识产权保护: 风险识别和规避[J]. 法学, 2023, 11(1): 143-155.
DOI: 10.12677/ojls.2023.111021

puts forward that a triune risk-aversion mechanism of "legal regulation + policy monitoring + technology autonomy" should be constructed to improve the efficiency of intellectual property protection.

Keywords

Blockchain, Intellectual Property Right Protection, Risk Identification, Risk Aversion

1. 引言

区块链是集分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型互联网应用模式。作为信息技术体系的革命性变革，被认为将成为继蒸汽机、电力、信息后，又一项影响人类社会和商业发展的重要技术之一[1]。目前区块链已经延伸到了金融、物联网、能源、教育、供应链管理、医疗以及司法存证等多个领域，并在知识产权保护中具有广泛应用前景。基于其强大的技术发展潜力和应用前景，区块链成为各界关注的热点。

2. 研究综述

目前区块链相关研究成果丰富，随着技术的不断发展和推进，不同时间段呈现出不同的研究热点。早期学者侧重于研究区块链的技术原理和技术特征，包括从区块链设计的密码学原理、共识算法、数据存储结构等方面来介绍区块链技术的基础架构[2] [3]，以及不可篡改、可溯源、智能化、去中心化、去信任化、透明化等技术特征[4] [5]。随后学者发现并论证了区块链在医疗、供应链、金融、政府管理、知识产权保护等诸多场域的适用性[6] [7]。与此同时，学者们还研究了区块链风险及其预防等问题[8]。

关于区块链和知识产权保护研究，目前大多数学者多基于区块链的技术特征，分析区块链运用于知识产权保护场景的可能性。区块链去中心化、抗篡改性、智能化等技术特征，可降低版权人交易成本和潜在维权成本[9]。基于哈希的分布式认证算法和信誉值的反盗版机制，阻断数字出版物盗版传播[10]；共享机制能够统一版权滥用标准，难以篡改的性质能够防止版权滥用，实现版权的反向保护与充分利用[11]。数据可追溯性、可拓展性和包容性，能解决专利运营中确权耗时长、用权变现难、不完全合同问题以及信息披露悖论等问题[12]。区块链分布式特征能够减少人为干预和操作的可能性，增强专利审查的公正、透明和权威性[13]。区块链的时间戳、不被随意篡改，可实现商标识别功能和商标公示功能[14]。供应链管理和追溯可以为预防商标侵权提供技术支持。也有少部分学者发现区块链在知识产权保护中的不足：匿名性等特征在降低版权保护成本的同时，也可能增加侵权行为[15]；以智能合约为基础的版权监管存在瑕疵，区块链与传统版权法律不匹配[16]。

简要评价。总体而言，目前研究取得了很大进展，但还存在如下局限：1) 从研究内容看，技术理性研究多，法律理性研究不足。已有文献偏重于分析区块链赋能知识产权保的技术特征，疏于研究技术理念和法律规制等外部要素的逻辑悖离困境，无法规避因区块链与法律的不兼容乃至冲突而导致的外部风险。2) 从研究视角看，技术性论证居多，风险防控研究不足。目前研究主要集中在论证区块链赋能知识产权保护的契合性，而其中潜在风险的相关研究比较零星、琐碎、缺乏系统性。区块链赋能知识产权保

护过程中优势与风险并存，犹如硬币的正反两个方面并存，面临数字虚假、数据霸权、信息泄露以及知识产权等风险。如不能识别、规避这些风险，将会大大削弱区块链的技术红利，不利于通过区块链提高中国知识产权保护的智能化水平，进而降低知识产权保护的整体绩效。本论文聚焦于区块链赋能知识产权保护中的风险问题，通过风险识别，构建风险阻断机制，以促进区块链在知识产权保护中的有效应用，凭借“技术自治”提高中国知识产权保护效率。

3. 区块链赋能知识产权保护的风险样态及其演化机理

总体而言，区块链的技术特征与知识产权保护的需求具有契合性。数字时代下，知识产权保护领域存在侵权频繁、确权难、交易难和维权难等痼疾。区块链为知识产权保护提供了新思路和新方法。首先，从技术角度而言，区块链的技术特征与知识产权保护的需求具有契合性。基于区块链具有去中心化、抗篡改性、可追溯性、公开透明等特征，依据时间戳及链式结构的电子存证记录方式，能够对知识产品进行即时确权、公开用权、定位侵权，不仅可以实现对知识产品的产权标引，解决知识产权保护实践举证难、确权难、维权难的三大痛点问题，还具备降低成本、安全可靠等优点。其次，从实践层面而言，区块链促进了知识产权保护的智能化。区块链证据及其规则初步形成，司法存证逐步融入实践而现实中，2018 年，杭州互联网法院区块链司法存证的采纳，为区块链赋能知识产权保护提供了实践基础。

然而，作为数据集成平台的区块链蕴含着各种风险：技术短板或者漏洞产生的内生性风险，以及法律、政策等社会要素引发的外生性风险。论文将区块链赋能知识产权保护的风险因素和风险源进行判断，将主要风险划分为如下几种类型：法律风险、信息风险、监管风险和知识产权风险。

本部分研究区块链引发各种风险的技术机理，包括：不可篡改性影响法定修改权的实施；去中心化挑战监管趋中心化原则；自动化执行无法避免非法后果，影响行为人真实意思表达；算法攻击和去信任化失灵导致的“数据独裁统治”；匿名性导致监管难；开放性难以保证数据上链前的真实性；技术漏洞导致的个人隐私外泄；非同质通证的发行引发知识产权冲突；等等。风险演化机理如图 1 所示。

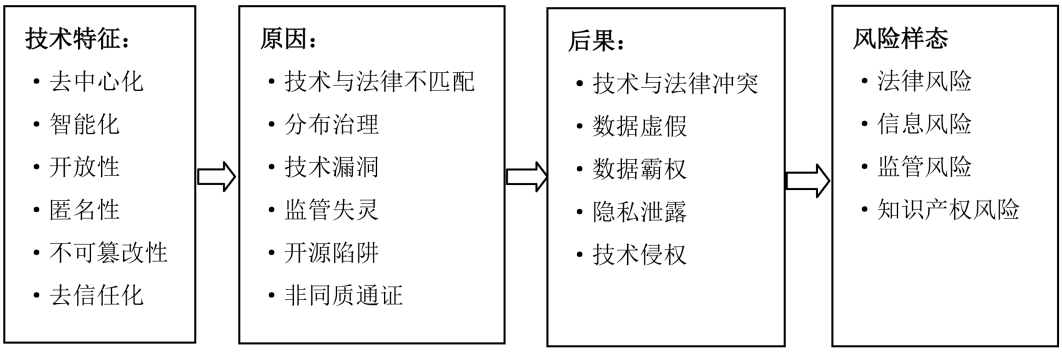

Figure 1. The risk generation mechanism of blockchain empowers intellectual property protection
图 1. 区块链赋能知识产权保护的风险产生机理

3.1. 法律风险

法律风险主要包括区块链的不可篡改性与知识产权修改权的冲突、智能合约的自动执行性影响真实意思表达、匿名性增加确认法律主体的难度、技术去中心化与法律趋中心化的矛盾以及开放性和匿名性带来司法困境。

3.1.1. 不可篡改性与知识产权的修改权相冲突

区块链具有不可篡改性，即信息无法撤回或删除，数据一经上链，就会永久性的储存在区块链中。区

块链的不可篡改性在知识产权保护中发挥着独特的应用价值，但与中国知识产权法定的修改权相冲突。在公有链中，数据被分布式储存在大量节点之中，每个节点只能修改本地数据，数据主体识别并要求所有储存其个人数据的节点更正或删除数据几乎没有可行性[17]。不可篡改性与知识产权主体在特定情形下的信息修改或删除权相悖的。中国《专利法》第 33 条规定：专利申请人可以对已经申请的专利文件进行修改；第 37 条规定，申请人应国务院专利行政部门的要求对其专利申请的修改。修改的原因不一，包括需要重新计算数据或者修改表达方法，或者使文件更清晰、准确，等。中国《著作权法》也明确规定了著作权人的修改权，即修改自由。此外，著作权权利也会因法院对于著作权纠纷裁判的影响而改变。而区块链不可更改的特性使知识产权人丧失了作品的修改权，导致知识产权权利无法得到有效且完整的保护，从而陷入了严重的逻辑困境：区块链的不可篡改性能解决溯源问题，从而解决确权难的问题，提高知识产权保护效率；然而，不可篡改特性使得权利人无法行使修改权，成为阻碍权利人的技术障碍。技术的不可篡改性与法定修改权产生冲突，导致技术促进知识产权保护和阻碍知识产权保护正负效应并存的悖论。

3.1.2. 智能合约的自动执行性影响真实意思表达

基于区块链的底层技术，智能合约具有自动执行性，其运作方式是：以计算机程序代码形式承载合约内容，在满足触发条件之时自动执行，无须引入第三方进行干预。执行性的优点在于：能够最大程度的保障合同正常运行，进而减少交易成本：缺点在于：无法变更与终止执行知识产权合同，特定情况下可能带来非法或者违法的法律风险。例如，知识产权人无法根据现实环境的变化调整其合约行为，当知识产权交易由于胁迫、重大误解、欺诈等因素，可能出现非法或者违法的后果时，无法及时调整或终止。智能合约自动执行的技术构造不将当事人情势变更、不可抗力等外部因素纳入考虑范畴，只会机械的执行相关程序，使得法理人情与技术代码分离，执行过于机械化、程序化，缺失了情理空间，也不可能如传统合同那般可以提前解除或者提前终止。这显然影响了知识产权人的自由意思和真实意思表达，也无法避免可能带来的不良法律后果。

3.1.3. 匿名性增加确认法律主体的难度

Filippi (2018)发现，区块链的匿名性与加密手段会引发诸多法律问题，包括：无法判断匿名当事人的法律能力，一方当事人或许会在不了解情况的前提下和没有民事行为能力的当事人签署智能合约，使得合约无法成立而面临损失；而且如果合约当事人一方或多方匿名，当执行合约存在失误时，由于难以判断匿名当事人身份，而导致受损一方不能借助法律等渠道寻求救助，尽管在当事人缺席状态下可以做出有利判决，但或许也会出现由于不能明确匿名当事人身份而造成判决无法真正落实的情况[18]。虽然著作权人可以使用自己在区块链上的身份进行作品的版权登记，但是一旦进入到维权环节，著作权人为了证明自己就是区块链上的这个主体就势必需要量明身份或者进行自证。这与区块链上的普遍匿名性存在一定的冲突[19]。匿名条件下，法律纠纷中有关人员的真实身份和违法证据难以确认，因而难以实施有效的法律约束。

3.1.4. 技术去中心化与法律趋中心化产生矛盾

区块链去中心化代表着解决多方信任问题的途径主要是通过算法和激励机制[20]。智能合约甚至可以支撑知识产权众筹、知识产权融资、知识产权交易引用代币制度而实施的知识产权评估等活动。“智能合约这种技术自动化极高，实际意味着支持自由市场和不信任集中权力。”[21]这种根本不受法律制度和政府政策约束的自助方式可能会利用程序设定中的漏洞达到非法目的，去中心化交易模式下的监管缺位也会使得智能合约的合法性受到质疑，违背智能合约设立的主旨，损害投资者的利益，造成公共秩序的混乱[22]。智能合约无法识别知识产权交易过程中是否有违反市场公平性原则的情况出现，其自动执行性即使造成产权转让中被不公平对待一方的损失，且受害者无法使用现有的法律规定内容作为依据请求法

院或仲裁机构变更或撤销合同。2016 年，黑客攻击 The Dao (一个分布式自治组织)代码里的漏洞，采取与代码运行模式相符的操作方式，将众筹中的资金转入自己的私人账户，导致用户财产的大量损失[23]。2017 年，智能合约平台 Parity 多重签名钱包也发生过两次安全事件，黑客给有漏洞的智能合约发送了两笔交易，目的是要获得权限和全部资金，最终造成 3000 万美元被盗和 1.5 亿美元在合约中无法取出[24]。黑客转移资金完全是按照智能合约中的程序设定的行为实施的。区块链的这种基于智能合约的去中心化运行机制，如果缺少强有力的规制主体、没有第三方规制机构参与，存在较大风险。一般技术规制与法律监管是趋中心化的，而且趋中心化可以在汇总优化当前制度资源和提升管控效率方面发挥一定作用。区块链依赖去中心化的运转模式与知识产权监管的中心化要求存在冲突。

3.1.5. 开放性和匿名性带来司法困境

司法困境包括两个方面：第一，司法管辖权困境。区块链公有链上的数据是公开透明的，它使得整个世界连成一体，形成了一个无国界的社会共同体。任何国家、任何地区的人都有机会获得、交流和传递信息。通过区块链，文学艺术等作品可以销售到全球各地，商标所有者能在世界范围内积累商业信誉，专利产品也能在全球范围内广泛传播。传统地域性司法管辖的依据，比如居住地、财产所在地、行为实施地等，都能与固定的物理地点一一匹配起来。区块链具有的开放性极大的削弱了地域性，传统的管辖规则在区块链中适用时遇到了很多障碍。权利人和侵权嫌疑人可能属于不同国家或地区，侵权行为发生地没有明确的地理标志。区块链发生的侵权行为，其司法管辖权归属于谁，目前法律没有明确规定。第二，全球保护难困境。由于匿名性特征，缺乏区块链上各种主体的真实身份的考证，导致侦查机关的侦查和取证工作开展难度大。而全球范围内受害者保护难度更大；由于开放性特征，各国法律体系存在差异，导致跨域国界的知识产权保护中可能出现犯罪认定标准差异大的情况，从而产生保护力度和水平不一的结果。

3.2. 信息风险

信息风险主要包括信息泄露、信息虚假、信息垄断等类别。

3.2.1. 非对称加密算法等原因引发信息泄露风险

本研究认为信息泄露风险的技术原因有三：1) 非对称加密算法。区块链采用“公钥 + 秘钥”对链上的信息进行非对称加密，一旦私钥保护不当或者账户失窃，权利人因难以找回就可能会完全丧失了对链上信息的控制权，链上的信息包括用户隐私和知识产权交易信息将存在泄露的风险。2) 匿名性和公开性。一方面，区块链的匿名性质允许人们在点对点的基础上进行交易，而不向任何人披露自己的身份。另一方面，基于公开性和透明性，任何人都可以检索在区块链上执行的所有交易的历史，并依赖大数据分析来检索潜在的敏感信息[25]。使攻击者能够轻而易举的获取链上信息，并通过获取的数据窥视到更多隐私信息。区块链中可以将知识产权领域中个体的信息资料转化为数据形式，随时被收集、使用、传播。这对个人数据信息安全构成了威胁，并对个人隐私数据的自治性和主动权形成了挑战[26]。3) 技术短板或安全漏洞。代码瑕疵、代码漏洞以及毁约丧失等问题，是区块链固有的技术问题。智能合约的安全漏洞，无法避免系统被攻击。智能合约就是一段计算机编码，编写程序存在漏洞或者技术短板。智能合约是通过事先预定、按照约定进行执行的，一旦满足触发条件，合约便会自动执行；且因为不可篡改性原因无法修改。正因如此，智能合约的漏洞一经发生，这种安全漏洞也无法终止执行，更无法进行修补。进而导致知识产权相关信息泄露。

3.2.2. 去信任机制失灵产生信息虚假风险

区块链有效赋能知识产权保护的前提是：上链数据的正确性、真实性与有效性。然而，“现有的区块链应用假设信任单一节点输入，这可能导致虚假或错误数据输入的问题。”[27]个别嵌有错误数据的恶

意或者不诚实节点的接入是不可避免的，可能导致被错误记录的数字知识产权资产存储或者交易的混乱[19]。基于类似共识机制失灵，可能出现虚假或者错误信息上链的情况。例如，行为人对音乐作品进行音轨剪辑又上传至区块链，造成无法准确判断侵权作品与原作品的“实质性相似”[28]，进而导致侵权证据真实性不足等。在版权保护应用方面，区块链的时间戳只能证明上链时间，但是无法验证信息在上链之前的真实性，而目前缺乏救济措施，因此难以有效打击盗版。

3.2.3. 算法难以避免数据垄断

由于算法模式、节点不足，或者授权机制等原因，会导致信息霸权和数字垄断。算法可能导致数据垄断，有三种途径：1) 算力攻击。量子计算使得区块链底层依赖的哈希函数、公钥加密算法、数字签名技术的安全性受到了威胁[29]，能破解基于加密算法构建起来的网络系统。算力攻击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[30]，从而产生数据霸权和垄断。2) 价值偏好。区块链的算法不是完全价值中立的技术活动，而是蕴含着某种价值判断[31]。区块链去中心化的特质理论上保证所有参与者平等[32]，这个问题引发了学者的质疑。如果不是所有参与者都平等，那会有利于哪个相关主体？是知识产权数据生产者还是数据管理者，是知识产权创造者还是使用者、传播者？不同利益主体是否会为了争取网络控制权而发生冲突？这些问题难于通过区块链技术本身来解决。利益集团的操纵、利用算法同样可能导致垄断、产生数据鸿沟，在多元参与者之间产生了公平性和合法性的问题，也可能增加知识产权数据的不真实性和不合理性。3) 区块链的运行机制。目前国内外最广泛使用的联盟链，存在不足：“一是联盟链的授权机制阻止大多数人访问权利的数据，会严重影响信息的透明公开；二是联盟链处于运行它的组织维护治理之下，具有不同程度的中心化性质，会影响公信力。”[33]因此可以推定：联盟链通行的授权机制和组织治理方式，易滋生数据垄断。

3.3. 监管风险

监管风险主要表现为监管呈分散性形态以及责任主体的查证难度增加。

3.3.1. 去中心化导致监管呈分散性形态

区块链呈现分布式、多节点的数据结构，与现有的区块链监管体制存在逻辑冲突。首先，去中心化使监管对象呈分散性。作为一个分布式的共享数据库，所有的节点都分散在数据库中，节点数量多且分散，导致无法有效直接而全面的管控，因而弱化了传统中心化的监管力度。其次，去中心化使监管主体呈分散性。去中心化意味着确权、维权、交易等行动可以在不同节点同时展开，而这些知识产权行为将涉及不同的主体，包括工信部门、市场监管部门、知识产权管理部门以司法系统等。由于监管对象、监管类别以及监管司法管辖权等方面的原因，区块链赋能知识产权过程中监管主体呈现分散性状态。区块链上知识产权保护的混业管理局面，其结果是导致监管层与层之间的交流不顺畅，且存在多重监管、监管空白、监管推诿、监管套利等监管漏洞。

3.3.2. 匿名性增加责任主体的查证难度

区块链的匿名性 + 加密性，使得难以确定法律责任主体，增加了知识产权保护中查证、追踪以及惩戒的难度。Neuburger (2018)发现：区块链可能会带来侵权行为，尤其是在匿名性特征下的匿名交易中，这种加密以及不可篡改的分布式系统下，非实名制的技术娴熟者会成为权利人的噩梦，有必要对该技术加以规制[34]。区块链匿名性带来两个难题：第一，用户信息形成非实名制的节点，而节点人格与法律人格并非一一对应。区块链用户的信息不再是自然人的真实信息，而是通过匿名化处理，形成非实名制的节点，一连串的数字代码就是它的表现形式。系统内的用户被转化成节点和数据，属于技术上的人格化，使得法律人格与节点人格并非一一对应。承担责任的基础是有明确的责任主体，而节点难以充当作法律

上的主体。第二，无法证明权利人和使用人是否一致。分布式的账本中不存在各个节点参与者的真实信息，所以无法判断权利人和使用人是否存在一致性。用户匿名参与知识产权交易，账户的作用也仅是承载完成交易的数字地址，并不显示真实的交易身份。用户双方的交易关系在区块链中被转化为数据地址之间的交易关系，造成主体形态和行为能力无法辨别。参与节点隐私的保密要求，知识产权交易双方真实身份无法确定，知识产权交易信息与真实身份信息的弱相关性。匿名性的这两个难题，其结果就是导致难以取证，难以确定法律责任主体。相关部门难以监控不法分子冒名顶替交易者的身份信息或者捏造虚假的身份参与交易。

3.4. 知识产权风险

知识产权风险主要表现为知识产权被抢注风险和知识产权侵权风险。

3.4.1. 知识产权被抢注的技术机理

1) 区块链的时间戳只能证明上链时间，无法证明知识产权真伪。区块链采用数据块加链式结构将知识产权信息保存在区块上，通过加盖一个不可更改的时间戳，以记录数据上链以及区块形成的时间。时间戳能够记录某人在特定时间对特定文件的访问，通常认定首个访问文件者就是其原创者。时间戳只能证明上链的时间，而不能保证谁是真正的知识产权的权利人。区块链的这一特性无法遏制知识产权被抢注。2) 区块链的开放性和匿名性，无法识别上链前信息的相似性。“区块链的开放性和匿名性事实上也可能增加侵犯知识产权的行为。人们可以通过区块链获得由权利人公开的部分知识财产信息，他们可能将其进行部分修改，然后重新上链注册。”[15]区块链只能够对已上链的内容实施溯源、跟踪和侵权监测，对于上链之前信息的真伪、来源以及相似性无法识别。因此无法避免知识产权抢注风险。

3.4.2. 产生知识产权侵权风险的主要原因

1) 非同质通证的发行。非同质通证是区块链应用的重要创新。“同一个作品可以用于生成多个非同质通证，各个非同质通证的发行方都可能声言其为唯一的、原创的来源；作品的所有权人和著作权人也有可能将不同的权利分别配置于不同的非同质通证中发行(理论上甚至可以分割所有权或著作权的不同权能而发行多种非同质通证)。”[35]这种风险即知识产权冲突。最先完成上链的作品存在知识产权缺陷，发行非同质通证可能通过公链的金融杠杆效应被不断放大，将增强因知识产权侵权引起的损害。2) 区块链的开源代码授权带来的问题。这是指区块链技术本身可能存在知识产权侵权风险。在开源成为新技术发布的首选方式和流行趋势的背景下，全球主流区块链架构均在开源平台进行了代码开源。开源软件与开源代码的风险来自内部风险和外部风险两方面。从内部风险来说，分两种情况：知识产权权利人有明确的授权，后续使用者自动获得免费的许可，在开源许可协议准许范围内使用或者在其基础上修改、编写程序代码，因此并不侵权[36]。但是，部分开源许可协议对授权没有明示，因而增加了后续使用者知识产权侵权风险。就外部风险而言，主要是来自指在自当不受开源协议约束的第三方的风险，当第三方拥有某软件知识产权，开源软件的原始开发者或者后续的修改者在程序或其衍生品上使用了该项技术，那么将可能面临侵权[37]。知识产权风险会阻碍区块链在实践场景中的广泛运用。

4. 区块链赋能知识产权的风险诱发因素

区块链赋能知识产权的风险诱发因素包括技术短板或者漏洞等内生性要素，以及法律、政策以及监管等外生性要素。

4.1. 制度供给缺陷

制度供给缺陷主要表现为制度缺失、与知识产权法律制度的冲突以及与合同相关法律互不兼容。

4.1.1. 制度缺失

1) 高位阶立法缺失。关于区块链技术存储数据是否属于电子数据，实际操作中很长一段时间没有得到明确的法律确认。直到2022年区块链证据才首次被纳入制度规范体系。2022年最高法发布《人民法院在线运行规则》，首次规定了区块链存证的效力范围，并确立了区块链存储数据上链后以及上链前的真实性审核规则[38]。总体而言，高位阶法律供给不足。2) 地方配套制度缺失。中国法律服务网“国家法律法规数据库”检索发现，2016~2022年，涉及区块链赋能知识产权保护的相关内容仅7部地方法规。梳理不同省市的知识产权保护条例内容，概括出区块链赋能知识产权保护的三种场景：将区块链的电子存证用于知识产权的行政和司法保护(辽宁省、海南省、江苏省)；依托区块链提供知识产权创新公证证明和维权取证等公证服务促进社会治理(海南省、上海市)；提倡知识产权保护部门加强运用区块链推动知识产权监督管理方式创新(山西省、上海市)。因此可以看出，中国地方目前对于区块链赋能知识产权保护的制度建设仍然相对滞后且制定缓慢。3) 知识产权权益受损后的救济制度缺失。工信部发布的《区块链参考架构》和《中国区块链和应用发展白皮书(2016)》都只是从技术层面对区块链进行规定，而没有提到权益救济。《区块链信息服务管理规定》只提到了对违反法律的信息服务使用者，可依法采取限制功能、关闭账号、警示等处置措施，也并未涉及平台使用者权益的保护[39]。知识产权交易或者运营过程中，由于救济制度的缺失，导致无法由于私钥丢失或者智能合约自动执行导致的权益损害无法得到有效弥补。

4.1.2. 区块链与知识产权法律制度的冲突

主要表现为：1) 区块链抗篡改性与著作权的修改权相冲突。区块链记录的时间戳与著作权的自动取得模式相冲突；区块链记录的抗篡改性与著作权的修改权互相矛盾，影响修改权的实现。2) 区块链的去中心化与知识产权的集中化管理方式违背。专利的集中化管理，需要利用公权力将分散在各专利权人手中的专利汇集起来，而区块链的诞生正是为了弱化公权力的约束与限制，因此两者产生冲突。此外，基于成本与收益比较，目前中国实施版权的集中管理制度。“对于面向数字版权保护而构建的区块链网络设计程序、系统运行的规则，目前法律并无相关专门规定，只能根据网络的创始人和技术的开发者根据自己的理念设计内部治理框架并选择相应的数字代码实施。区块链技术运行的去中心化设计理念与国家官方机构的集中管理制度存在矛盾。”[16]

4.1.3. 区块链智能合约与合同相关法律互不兼容

学界对于区块链智能合约的法律性质存在两种相反的观点：多数学者主张智能合约即是法律合同。智能合约是区块链的底层技术，其原理是通过达到程序中预设的条件来自动执行合同，其中设定的代码相当于合同条款。在知识产权保护中智能合约可在数字版权交易和知识产权众筹等过程中发挥作用。智能合约符合合同的本质出发，是当事方之间关于建立或改变权利义务关系的合意。只要能够体现各方达成合意，无论是书面形式还是代码形式均不影响合同的成立[40]。少数学者认为智能合约与合同要素并不完全一致。智能合约只是法律合同的一种履行方式，本质上就是一段代码或数字程序，并非合同内容，缺乏合同的一般要件，如合同形式、终结及适用法律等条款[41]。智能合约仅仅是一种新型的自助行为，执行合同的程序代码，不具备作为合同本身的法律地位[42]。“目前《民法典》合同编没有把智能合约列入其中，也没有将其作为‘不完全列举的合同类型’”[43]。这体现了智能合约在法律中的模糊地位以及其与法律的不兼容状态。

4.2. 区块链存在技术短板或者漏洞

区块链存在技术固有特征及漏洞且技术机理难以精准作用于实践。

4.2.1. 技术固有特征或漏洞

以隐私泄露风险为例。隐私泄露的主要原因有技术固有的特征、合约漏洞等。区块链具有去中心化、公开性和匿名性，本身容易导致隐私暴露，途径有：比较比特币交易图谱可获取用户行为统计特征，通过比特币找零地址可推算出客户交易数据，通过分析等隐私数据。合约的漏洞来自三个方面：不同的编程语言因设计缺陷各不相同，可能会存在变量覆盖、未校验返回值、拒绝服务等不同的漏洞；开发者编写代码质量的不同，引发的漏洞；虚拟机或容器等运行环境，导致运行机制方面的漏洞[44]。此外，技术风险还来自于算法和恶意攻击等。例如，区块链环境下量子计算引发的算力风险，会强化知识产权证券交易中某一方不公平的数据垄断优势与算法歧视，可能无意间为专利、商标的抢注带来便利[45]。这在某种程度上助长了“专利流氓”现象的扩散，增加了政府监管的技术难度。

4.2.2. 技术机理难以精准作用于实践

区块链共识机制的种类较少，难以匹配多样化的应用场景，而且，当前对跨场景和跨平台的跨链技术的研究较为薄弱，其技术机理与业务需求精准对接的实践应用尚不够深入、成熟。例如在版权方面，区块链无法通过算法来认定作品是否满足“独创性”要素(目前中国司法实践中对于作品“独创性”要件的争议，都是由法官从主客观两方面认定的)，也无法验证信息在“上链”之前的真实性，因此也难以打击盗版。对于商标和专利权，由于需要经过审核，基于区块链的时间戳目前只能作为一种辅助工具。当采用时间戳以及数据节点进行著作权保护时，如果无法科学合理地控制节点范围，会造成技术垄断或者思想僵化的问题，阻碍知识产权市场的良性发展。

4.3. 监管体制不完善

产生监管风险的原因：第一，区块链去中心化的特征，弱化了传统中心化的监管模式。增加了监管的难度，使得难以对整个行业进行有效规制。第二，技术处于发展期，缺乏统一的监管标准。法律责任主体难以明确，由于使用者的自由进出机制导致公有链的具体法律主体难以认定；联盟链和私有链尽管责任主体明确，但基于其“部分去中心化”的特性，难以明确规定平台服务商、使用者和平台三者之间的责任。第三，缺乏统一的监管部门。目前中国监管体制是按照传统分业监管模式授权各监管部门在各自所涉及的信息产业领域内进行监管，区块链企业的注册登记等由市场监督管理局负责；信息数据方面由信息化部门负责；等等。区块链赋能知识产权领域呈现多头管理现象。第四，监管措施不足。目前在区块链中发挥作用的数据信息法律侧重于监管数据的收集，也就是对早期的过度收集数据行为进行了规范，而在数据的后续利用和流转方面却缺少监督。另外，区块链本质上是一套治理架构，其核心是基于多种技术组合而建立的激励约束机制。现阶段政府部门只是作为区块链政策的制定者，没有投入到区块链应用场景的管理中去。对区块链赋能知识产权保护的监管措施也只是单纯进行违规打击，而没有进行正确的合规引导。

5. 区块链赋能知识产权的风险规避路径

本部分从管理和技术两个层面，探索“法律规范 + 政策监控 + 技术自治”三位一体的风险防范机制。

5.1. 优化法律规范

5.1.1. 构建包容性的法律框架，弥补智能合约法律空白与漏洞

针对智能合约的不可篡改性、自动执行性可能带来的法律风险，首先必须完善智能合约的相关法律界定和法律救济制度。可以遵循如下途径：第一，承认智能合约的法律地位，将智能合约纳入法律体系。可将智能合约纳入《民法典》、《电子商务法》、《网络安全法》、《电子签名法》等法律框架内，设

立专门智能合约的约束条款；第二，完善救济制度，包括明确现行制度中有关智能合约修改、解除、履行等的制度安排，以及规定智能合约中各种主体法律、法律责任以及被侵权时的救济措施等内容。

5.1.2. 完善数据相关的法律体系，加快数据安全的立法进程

针对区块链匿名性和开放性带来的信息风险，应该加快对数据安全、隐私保护、网络安全等法制薄弱领域的立法进程。可遵循如下途径：第一，明确数据权利的法律地位。在个人信息安全的法律体系中，明确区块链相关的个人数据控制权，以及个人数据的合规性、合法性。第二，完善数据保护法律。可借鉴欧盟《一般数据保护条例》的经验，明确规定个体数据使用边界、数据权限、数据监管处理的主体与程序等事项[46]。确立个体隐私安全保护的法律规范。第三，构建私钥法律体系，加强密码的法律保护，以保护链上知识产权数据信息安全。“哈希函数、非对称加密、公钥和私钥都属于加密的方式，都达到了‘去标识化’的要求，因此个人信息无论通过哪种方式，只要不是明文方式上链，都可以视作达到个人信息保护规范要求的‘保密’要求。”[47]构建私钥法律保护体系，应该明确规定盗窃私钥的个体责任以及平台责任以及救济手段等事项。

5.1.3. 实现代码与法律互补，促进技术自治与法律规制的融合

将科技应用于法律领域，作为法律实施的辅助机制。通过“代码助法”，实现区块链对法律的优化和升级[23]。技术能够弥补法律或者取而代之，但技术代码和法律都有其固有的缺陷，单方面治理都存在很大的局限性，融合治理才是最好的解决方式[48]。法律和技术代码应当是相辅相成、优势互补的关系。但技术与法律的融合并不代表着两者的规范效力处于同等地位，还要遵循主次分明的融合理念，应当以法律规范为主、技术代码规范为辅。融合途径如下所示：第一，以法治链。建立计算机语言转化和条款审查标准。将链上公约规范化、标准化，形成链上法则，对上链、交易及下链等程序作出严格规定，并将其代码化，使其成为区块链系统的一部分，最终构建监管机制，实现技术与法律的融合。第二、以链治链。运用区块链的自我监管功能，实现链上秩序的治理。国外学者提出不同的“以链治链”思路：构建“多中心共同监管”模式，即通过将区块链系统中的各种主体纳入监管的设计、构建和实施中，从而将区块链自我治理能力纳入监管框架[49]；实施“内生监管”模式。监管者与区块链生态系统成员合作，将合规性植入区块链技术的底层协议中，并通过迭代过程推进监管的不断完善[50]。“以法治链 + 以链治链”可实现从法律和技术双重角度解决区块链风险预防问题，保护知识产权保护中各方主体合法权益。

5.2. 加强政策监管

5.2.1. 构建多元主体监管体系

多元主体监管体系包括：政府监管、行业监管、平台监管。途径如下：第一，明确政府监管主体，理顺政府监管体制。明确具体的监管部门，由工信部综合监管区块链上的知识产权行为，其余和区块链技术相关的各部门如市场监督管理局、国家互联网信息办公室等在服从统一管理安排的基础上通力协作、分工配合，共同监管平台供应链上的商流、物流与资金流[51]。主次分明的监管主体结构有助于法律约束力的提高，能明确各监管部门的职能分配，从而提高监管的效率。第二，完善行业自律机制。重视区块链知识产权保护中行业协会及创新服务企业等自律组织的作用，包括：制定行业规则，完善数据上链规范、私钥管理规范、节点监管规范等；促进区块链标准化建设，为监管提供标准支撑；等等。第三，加强区块链平台监管。包括优化平台的准入制度，严格设置区块链平台企业、从业人员以及区块链平台使用者的准入要求等等；明确平台知识产权相关数据审核、建立清理机制、规范用户使用平台的权利和义务，以及确定侵权责任平台分担等事项。

5.2.2. 创新监管方式

可引入“监管沙盒”(Regulatory Sandbox)的监管模式。该模式属于金融科技，是英国金融行为监管局首创，指：“一个‘安全空间’，企业可以在其中试验创新产品、服务、商业模式和交付机制，而不会立即产生正常情况下从事相关活动的所有监管后果。”[52]引入“监管沙盒”的优点在于：第一，通过降低准入门槛，让知识产权相关主体充分创新知识产权产品、服务、商业模式和交易机制，并且能够避免区块链平台创新的测试风险向用户转移。第二，营造一种较为自由的空间，在兼容性的框架下，包括区块链平台、知识产权创作者 E 及使用者等在内的有关主体可以获得监管机构赋予的更多权利。因此，把“监管沙盒”运用于区块链监管，既能满足政府弹性管理，又能有效促进政府与监管对象间的合作，还可以保护创新知识产权保护机制的用户。

5.3. 实施技术自治

针对技术短板和数据垄断等风险，应该寻求技术自治途径，在加强重点技术研发的同时，促进区块链与其它数字技术的融合。

5.3.1. 加强技术研发，攻克区块链关键技术难题

应遵循如下途径：第一，强化区块链底层技术的基础研究，加强抗攻击能力。应该强化安全开发、代码审查、安全评估和测试等各个环节的研究，提升技术安全。例如，可研究并采取美国国家标准与技术研究院(NIST)发布的网络安全框架，以识别区块链的风险并加以控制。“由于区块链系统自身漏洞造成的黑客攻击防不胜防。NIST 网络安全框架明确规定区块链网络环境安全，尽管该框架不是专门为区块链技术设计的，但其标准足够广泛，足以涵盖区块链技术，并帮助机构开发识别和控制影响区块链技术的风险的管理系统和流程。”[53]第二，展开区块链重点发展领域研究，巩固“区块链 + 知识产权”产业发展的技术基础。应当积极寻求分布式账本、智能合约、隐私保护、非对称加密等关键技术的突破，为区块链赋能知识产权提供技术支持。第三，加强区块链的算法研究，破除数据垄断、数字鸿沟。从技术维度而言，应该从算法本身的运作入手、优化算法模型，所用数据的品质优化入手、避免数据偏见，以保证算法公正；强调算法公开，强化算法解释，推动算法祛魅[54]。“重新定义算法权力，将数据要素分布在自我治理的所有主体之中。分布式储存的数据不再集中于少数平台及少数人手中，以此纠正市场缺陷导致的市场失灵，构建更加公平的数据市场，消除数字鸿沟，从根本上破解垄断根源。”[55]此外，还应该争取技术话语权，避免算法垄断给中国知识产权保护带来弊端。

5.3.2. 促进区块链与人工智能、大数据等技术的联合

区块链与人工智能、大数据等技术存在密切的联系，技术间的融合必定会共同推动经济社会的进步。大数据算法可全网自动抓取信息，通过知识产权信息的数据分析与对比，设立知识产权风险预警和评估系统。人工智能技术在人脸与指纹识别、自动化程序、智能控制等方面的优势恰好可以弥补区块链知识产权信息上链前的不精确管理，锁定侵权主体，能破解上链信息虚假、匿名带来的法律主体确定难、外部技术攻击等困境。

5.4. 防范知识产权风险

5.4.1. 提高知识产权风险意识，率先知识产权布局，预防知识产权抢注

知识产权主体应该加强知识产权布局，积极申请专利、版权以及商标，以防被抢注，导致重大财产损失。尽管区块链有利于知识产权交易和运营，但是在目前而言，传统的知识产权保护体制仍然发挥着主要作用。因此，必须依托原来保护机制，即知识产权行政保护和司法保护为主，区块链技术自治和自力救济为辅。发现可能存在知识产权侵权的时候，可以借助于区块链取证、确权，从而实现维权的目的。

5.4.2. 治理非同质通证带来的知识产权冲突问题

“通过法律认可明确非同质通证的合法性边界；确定非同质通证的监管主体与职权职责结构。可探讨形成一种包括工信部门、网信部门、市场监管部门和知识产权保护部门等在内的层次化的职权职责结构设计；推动建立多种国家标准或行业标准，政府标准化建设部门要求非同质通证的发行、使用和流转，必须涵盖区块链交易追溯、权益证明、纠纷解决、合约审计等机制。”[36]通过主要法律机制、政府监管和技术标准化三种途径，从法律保障、政策监管和技术安全保障措施三个角度来约束非同质通证，减少知识产权冲突风险。

5.4.3. 警惕开源软件的知识产权侵权陷阱

从区块链本身而言，也要避免侵权，才能为赋能知识产权保护提供更好的技术平台。因此，必须做好区块链研发的前置工作——检索知识产权信息(申请或授权状态，有效或无效，等等)，把握开源软件的授权方式和尺度，避免落入开源软件的侵权陷阱。

基金项目

国家社会科学基金一般项目“知识产权保护中区块链应用的风险识别及防范机制研究”(20BGL007)。

参考文献

[1] Webb, A. (2015) 8 Tech Trends to Watch in 2016. *Harvard Business Review*, **3**, 20-21.

[2] 杨晓晨, 张明. 比特币: 运行原理、典型特征与前景展望[J]. 金融评论, 2014, 6(1): 38-53+124.

[3] 张偲. 区块链技术原理、应用及建议[J]. 软件, 2016, 37(11): 51-54.

[4] Wood, G. (2014) Etheruem: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, 1-32.

[5] Swan, M. (2015) Blockchain-Blueprint for a New Economy. O’Reilly Media, Sebastopol, 9.

[6] 李洪晨, 马捷, 胡漠. 面向健康医疗大数据安全保护的医疗区块链模型构建[J]. 图书情报工作, 2021, 65(2): 37-44.

[7] 李彦. “区块链+人力资源管理”在政府部门绩效管理中的应用与创新[J]. 领导科学, 2021(16): 71-74.

[8] 夏纪森, 臧志宏. 论区块链应用的社会风险与法律治理[J]. 常州大学学报(社会科学版), 2019, 20(1): 25-35.

[9] 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.

[10] 田园. P2P 内容分发网络的数字版权保护系统研究[D]: [硕士学位论文]. 北京: 北京邮电大学, 2012.

[11] 王力晓. 区块链技术在版权滥用领域的创新应用[J]. 对外经贸, 2022(5): 39-42.

[12] 汪亮, 曹锂, 刘芙蓉. 区块链技术在专利运营中的应用探讨[J]. 杭州科技, 2019(5): 36-38.

[13] 郭志强. 区块链技术在专利申请与保护业务中的应用研究[D]: [硕士学位论文]. 开封: 河南大学, 2019: 1.

[14] 张怀印, 凌宗亮. 区块链技术在商标领域的证明作用[J]. 知识产权, 2018(5): 76-82.

[15] 陈永伟. 用区块链破解开放式创新中的知识产权难题[J]. 知识产权, 2018(3): 72-79.

[16] 马明飞, 刘新洋. 区块链在数字版权领域应用的困境与对策[J]. 中国出版, 2020(9): 56-59.

[17] Finck, M. (2018) Blockchains and Data Protection in the European Union. *European Data Protection Law Review*, **4**, 17-35. https://doi.org/10.21552/edpl/2018/1/6

[18] Filippi, P.D. (2018) Blockchain and the Law: The Rule of Code. Harvard University Press, Cambridge, 371-372.

[19] 张辉, 王柳. 区块链下网络文学版权保护问题研究[J]. 法学论坛, 2021, 36(6): 116.

[20] 程雪军. 区块链规制的国际经验与中国策略[J]. 中国流通经济, 2021, 35(3): 31-43.

[21] Raskin, M. (2017) The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, **305**, 327. https://doi.org/10.2139/ssrn.2842258

[22] 华劼. 区块链与智能合约在知识产权确权和交易中的运用及其法律规制[J]. 知识产权, 2018(2): 13-19.

[23] 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, 19(3): 128-144.

[24] 探路人. 以太坊安全之 Parity 第一次安全事件漏洞分析[EB/OL]. https://blog.csdn.net/xuguangyuansh/article/details/80786691, 2022-09-01.

[25] Filippi, P.D. (2018) Blockchains and Data Protection in the European Union. *European Data Protection Law Review*, **4**, 26-27.

[26] 刘哲, 郑子彬, 宋苏, 等. 区块链存在的问题与对策建议[J]. 中国科学基金, 2020, 34(1): 7-11.

[27] 王醒. 一种基于智能合约的非金融资产数字化方法[D]: [硕士学位论文]. 广州: 暨南大学, 2018: 15.

[28] 黄武双, 邱思宇. 论区块链技术在知识产权保护中的作用[J]. 南昌大学学报(人文社会科学版), 2020, 51(2): 67-76.

[29] 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望[J]. 自动化学报, 2019, 45(1): 208.

[30] 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, 41(7): 85.

[31] 丁晓东. 算法与歧视: 从美国教育平权案看算法伦理与法律解释[J]. 中外法学, 2017(6): 1609-1623.

[32] 赵金旭, 孟天广. 技术赋能: 区块链如何重塑治理结构与模式[J]. 当代世界与社会主义, 2019(3): 189.

[33] 王春霈. 基于区块链的知识产权保护技术的研究[D]: [硕士学位论文]. 哈尔滨: 哈尔滨工业大学, 2020: 22.

[34] Neuburger, J. (2018) Blockchain as a Content Distribution Technology: Copyright Issues Abound. https://www.blockchainandthelaw.com

[35] 苏宇. 非同质通证的法律性质与风险治理[J]. 东方法学, 2022(2): 58-69.

[36] 付娜, 李文宇, 毕春丽. 开源中的知识产权风险分析[J]. 世界电信, 2017(2): 42-46.

[37] 刘雪凤, 杨易婷, 张笑. 中国区块链产业的专利战略研究[J]. 法学, 2020(4): 600.

[38] 马明亮. 区块链司法的生发逻辑与中国前景[J]. 比较法研究, 2022(2): 15.

[39] 张雪. 我国区块链平台的法律问题研究[D]: [硕士学位论文]. 贵阳: 贵州大学, 2019.

[40] Werbach, K. and Cornell, N. (2017) Contracts ex Machina. *Duke Law Journal*, **67**, 340-341.

[41] Savelyev, A. (2017) Contract Law 2.0: "Smart" Contracts as the Beginning of the End of Classic Contract Law. *Information & Communications Technology Law*, **26**, 116-134. https://doi.org/10.1080/13600834.2017.1301036

[42] Raskin, M. (2017) The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, **1**, 333-335.

[43] 何士青. 基于法治主义维度的区块链智能合约发展研究[J]. 政法论丛, 2022(2): 48.

[44] 卫霞, 白国柱, 张文俊, 等. 智能合约平台安全风险分析及应对研究[J]. 世界科技研究与发展, 2022(10): 1-12.

[45] 戚学祥. 超越风险: 区块链技术的应用风险及其治理[J]. 南京社会科学, 2020(1): 88-92.

[46] 权雅之. 区块链技术推动法治建设的多重路径与应用前景[J]. 珠江论丛, 2020(2): 150.

[47] 王禄生. 区块链与个人信息保护法律规范的内生冲突及其调和[J]. 法学论坛, 2022, 37(3): 92.

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

[49] Finck, M. (2018) Blockchains: Regulating the Unknown. *German Law Journal*, **19**, 686-687.

[50] Reyes, C.L. (2016) Moving beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal. *Villanova Law Review*, **61**, 222-233.

[51] 杨慧琴, 孙磊, 赵西超. 基于区块链技术的互信共赢型供应链信息平台构建[J]. 科技进步与对策, 2018, 35(5): 21-31.

[52] Financial Conduct Authority (2022) Regulatory Sandbox. https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf

[53] 刘双印, 雷墨鸳兮, 王璐, 等. 区块链关键技术及存在问题研究综述[J]. 计算机工程与应用, 2022, 58(3): 77.

[54] 黄静茹, 莫少群. 算法监控的逻辑理路、伦理风险及治理路径[J]. 南京社会科学, 2022(6): 134.

[55] 武西锋, 杜宴林. 区块链视角下平台经济反垄断监管模式创新[J]. 经济学家, 2021(8): 81-88.