【文章编号】1002—6274(2022)01—151—10

区块链技术在商业秘密保护中的运用及法律规制*

邢玉霞[1] 宋世勇[2]

(1.山东政法学院民商法学院,山东 济南 250014; 2.齐鲁工业大学(山东省科学院)政法学院,山东 济南 250353)

【内容摘要】随着大数据与人工智能算法的迅速发展,区块链技术在保护商业秘密数据真实性方面显示出突出优势,但也面临公有链与联盟链形式的系统风险、区块链自身延展性价值实现不充分及对区块链高位阶法律规制不健全等各类风险。探索“标准共识兼容插件+多链并存与跨链兼容”模式、鼓励前置性商业秘密司法鉴定业务、完善区块链诉讼证据机制、加强对智能合约的法律规制等成为区块链技术保护商业秘密的必要选择。

【关 键 词】商业秘密 区块链 智能合约 证据存取 前置性司法鉴定

【中图分类号】DF523 【文献标识码】A

以中共中央政治局第十八次集体学习与第二十五次集体学习为标志,区块链与知识产权保护上升为我国国家战略重点;中共中央、国务院在 2021 年 9 月印发的《知识产权强国建设纲要(2021-2035 年)》进一步要求建设面向社会主义现代化的知识产权制度,加快大数据等新领域新业态知识产权立法,处理好数据开放与数据隐私保护的关系,充分实现知识产权数据资源的市场价值;国务院在 2021 年 10 月印发的《十四五国家知识产权保护和运用规划》中将“商业秘密保护工程”与“数据知识产权保护工程”作为第 1、2 号专栏予以强化,体现了商业秘密与区块链为代表的电子数据在知识产权强国建设中的重要地位。相比其他知识产权,区块链技术保护商业秘密问题更为典型。社会实践中,众多企业对商业秘密保护的畏惧感来自于保护的成本远远高于其收益,只有企业认为商业秘密应该保护而且通过保护措施可以实现其利益期望值,才会激发企业保护商业秘密的热情和持续动力。区块链技术去中心化、全程可追溯的天然优势决定了它能为专利、商标、版权、商业秘密和地理标识等知识产权提供更为完善的保障,但其自身的系统缺陷及相关法律风险同样突出,如何依法规范区块链技术保护商业秘密、实现其最大价值成为当前理论与实务界需要解决的首要问题。

一、法理基础:合法性是法定形式商业秘密首要构成要件

商业秘密属于《中华人民共和国民法典》(以下简称《民法典》)第 123 条规定的知识产权“7+1”类客体之一,这是中国在基本法律层面对商业秘密性质归属的定性,肯定了商业秘密适用知识产权保护的一般原理。当前国内理论学界及司法实务领域普遍认可商业秘密构成要件“三要件说”。依据《中华人民共和国反不正当竞争法》(以下简称《反不正当竞争法》)及《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》,商业秘密以技术信息和经营信息等商业信息为保护对象,必须具备以下三个要件:不为公众所知悉的秘密性——被诉侵权行为发生时不为所属领域相关人员普遍知悉和容易获得;商业价值性——包括现实及潜在商业价值,能为权利人带来竞争优势;合理性的保密措施——保密措施只需要与商业秘密的客观秘密性及商业价值性等实际保护需求相适应即可。

* 基金项目:本文系国家知识产权局软科学研究项目“商业秘密司法鉴定现实困境与规范化路径研究”(SS20-B-27)、2021 年度山东省人民检察院专题调研和理论研究重点课题“区块链保护商业秘密检察业务典型问题与对策研究”(SD2021B08)的阶段性成果。

作者简介:邢玉霞(1974-),女,山东威海人,山东政法学院民商法学院教授,研究方向为商法与知识产权法;宋世勇(1975-),男,山东高密人,法学博士,齐鲁工业大学(山东省科学院)政法学院副教授,通讯作者,研究方向为知识产权法。

从广义范围而言，商业秘密可以表现为自然形式的商业秘密与法定形式的商业秘密两个方面。自然形式的商业秘密属于企业等权利人主观认知的、实质意义上的商业秘密，包括合法与不合法等一切形式的商业机密信息，只有法定形式的商业秘密才能被依法保护。合法性是法定形式商业秘密的首要要件，对于商业秘密的认定与依法保护不可或缺。但是我国现行商业秘密相关立法并未将“合法性”作为商业秘密的“显性”必要构成要件，一般的理论探讨、行政执法及司法实践大多还是以上述“三要件”为对象，认为作为法律规制对象，合法性不需要独立讨论和对待。这种思维对于专利、商标等其他知识产权也许适用，但对于商业秘密而言，其权属一直处于不确定状态，是否合法、商业秘密权是否真实存在，在没有发生纠纷之前，只有所谓的商业秘密权利人主观认知，客观真实性无从确认。一旦发生商业秘密争议或纠纷，确权是首要程序，对商业秘密的合法性审查应是确权程序中的首要步骤。

司法实务中曾经发生过针对商业秘密合法性审查程序不统一导致案件审判结果迥异的典型案例[1]P107：依据上海市第一中级人民法院（2006）沪一中民五（知）初字第95号与上海市高级人民法院（2006）沪高民三（知）终字第92号判决书显示，安客诚信息服务（上海）有限公司与上海辰邮科技发展有限公司等企业之间发生了侵犯客户信息形式的商业秘密争议的情形。一二审法院对此作出了完全不同的判决：一审法院认为，以海量自然人个人信息作为公司客户名单的商业信息属于当事人商业秘密，应该得到保护；二审法院则以当事人未能举证其合法获取“海量自然人信息名单中的自然人”同意“将其个人信息作为企业客户名单”的证据，以证据来源合法性不足为由否认了此类客户名单属于商业秘密的可能性。本案二审法官裁判法理与英美衡平法中“手脚不干净者不得诉诸衡平”规定的“来源合法”之法理异曲同工，很好地说明了法定形式的商业秘密，无论是技术信息、经营信息或其他需要保密的商业信息，合法性要件（包括内容合法、来源合法等）不仅应成为商业秘密认定的行政执法与司法实践业务的首要审查要件，而且还应是理论构成要件中的首要考量要素。本判例发生在2006年，可以说二审法官的办案理念非常先进，因为一直到2020年《民法典》实施，才对自然人隐私权及个人信息保护在第六章作了专章规定（2017年实施的《中华人民共和国民法总则》仅在第五章第一百一十条和一百一十一条对隐私权和个人信息做了概括规定），2021年9月实施的《中华人民共和国数据安全法》与2021年11月实施的《中华人民共和国个人信息保护法》随后也对数据安全及个人信息进行了详尽规定。至此，个人信息与数据商用及作为专用客户信息使用具有了严格、明确的法律界限，企业再以海量个人信息主张为自己的商业秘密，对于来源与内容合法性的举证就成为必须，这对于推动行政执法与司法裁判尺度的统一具有积极意义。因此，商业秘密构成的“四要件”标准优于传统的“三要件”标准，更有利于准确认定商业秘密秘密点与商业秘密权。

二、应用基础：区块链技术保护商业秘密安全优势明显

2021年8月实施的《人民法院在线诉讼规则》是我国首次对区块链技术存储证据形式审查与核验作的最为全面的法律规制，体现了司法实践中区块链证据存储技术应用的现实广泛性、未来可期性与问题多发性。其实，区块链作为大数据、人工智能算法有机融合的电子数据类知识产权证据存储技术，除在金融、物联网等社会各领域广泛应用之外，在此前的司法实践中也早已被广泛推广。2018年杭州互联网法院审理的著作权案首次将区块链证据认定为诉讼证据，被视为中国司法实践全面应用区块链技术的开端。全国统一司法区块链平台也在最高人民法院主导下推广应用，创新了证据的在线存储方式，推动解决电子证据取证难、存储难、易篡改与认证难的问题，实现了由制度信任（由人主导的主观信任）向机器信任（由技术保障的客观信任）的转变，信任成本极大降低，信任效益极大提升。

（一）区块链可为商业秘密提供“零知识证明”安全保护，低成本实现商业秘密权利人的合理保密需求

随着大数据与人工智能技术的快速发展，商业秘密数据化保护正逐渐成为商业秘密权利人的优先选择。数据化实践拓展了商业秘密等知识产权的存储、交易方式，但同时也因数据化知识产权内容的获取方式表现为“所有人对所有人的传播”模式而发生了巨大变化导致风险剧增：载体的数字化与网络的虚拟

化,权利人难以控制自己的作品在多处复制和传播,更难以确定侵权因果关系及侵权人;同时网络技术使得数字版权侵权形式多样化,而多样化侵权形式并未全部纳入现行法律规范范围也会导致权利人向侵权人追究责任时无法可依[2]。

区块链技术被定义为“第四次工业革命”的核心技术,具有完整性、透明性、保密性和全程可追溯性的特点,在信息时代的重要资产——数字内容的交易环境下,能够很好地解决数据的非法复制、伪造及利润分配等典型问题。[3] 这一切也是人类在历史上首次创造出了不可复制和伪造的数据库,同时也不需要依靠任何第三方中心机构就可以独立完成身份验证。[4] P54 去掉中间环节,由商业秘密权利人直接将商业信息上链完成登记,区块链呈现的并非是商业信息本身,而是经过哈希算法加密后的哈希值,不会暴露其内容,实现了保密性的基本要求。[5] P120 因此,区块链为商业秘密提供的是“零知识证明”。[6] P561 后续关于这些商业信息的一切变动都完整呈现并可追溯,很好地解决了商业秘密的存续和保管难题。[7] 算法商业秘密的存在使算法处于“黑箱”之中,[8] 经过算法完成的哈希值保证了商业秘密权利人上链后商业秘密的秘密性,链上所看到的唯一信息是固定长度的代码及表明交易信息的时间戳。这种方式具有效率高、成本低、保密性强、可追溯等特点,很好地解决了商业秘密保密难、保护成本高的传统难题。以区块链技术保护商业秘密免除了知识产权的传统注册或确权的复杂和昂贵过程,打破了知识产权的地域性限制,并在确保商业秘密安全管理及区块链技术方或权利方直接面向用户收费等方面提供了全新的安全体系支持。用区块链技术保护商业秘密,在实现商业秘密的存储、取证、侵权鉴定等方面的电子证据最优化方面提供了更好的技术支持。

(二)区块链底层特殊存储结构优势有助于保障商业秘密稳定与安全

区块链技术依靠著名的非对称性加密算法技术,形成了其自身的典型特性,如抗篡改性和全程可审核性,[9] 或可表述为分散性、责任制及安全性[10] p69。在区块链存储技术中,以哈希值形式加密存储信息,保证的是信息内容的内在安全,其作为有效证据的外在安全稳定性,则来源于区块链技术特有的纵向与横向双重保障机制。纵向保障机制表现为持续扩容的链式结构,每一个区块中的哈希值均包含了本区块以前的哈希值及区块形成时间,单个或部分区块的自行更改难以实现。横向保障机制表现为区块链存储技术的多点分布存储机制,单点或部分点位的自行更改也难以被最终确认。随着电子数据形式的证据在诉讼中越来越广泛的应用,区块链技术的这一天然技术优势,很好地解决了电子数据诉讼“不稳定”“易篡改”的天然劣势,从而被《人民法院在线诉讼规则》确认并重点推广规范使用。在本规则关于电子数据证据的九条直接规定中(第十一条至第十九条),区块链的规定就占了四条(第十六条至第十九条)。相比 2018 年 9 月生效实施的《最高人民法院关于互联网法院审理案件若干问题的规定》只在第十一条电子数据审查“对区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存储平台认证证明其真实性应当确认”简单的单款规定,充分说明区块链技术存储形成的证据逐渐成为中国当前司法实践中的电子证据主流形式。正是区块链存储技术的纵向链式结构与横向多点式分布机制,保证了在此基础上形成的证据的稳定性与难以篡改性。

三、现实难题:区块链技术难以全链条保证商业秘密绝对安全

区块链作为一种开源技术出现,不属于任何的个体,[11] 区块链基于其数字内容的性质,其作者很难获得权利与对应的收益,同时还可能被恶意用户篡改数字内容,[3] 因此,区块链技术保护商业秘密也面临着诸多风险。从司法实践视角来看,商业秘密保护的难题包括商业秘密的确权、商业秘密被侵权、商业秘密被侵权后的损失计算等各方面。区块链过程的透明性、全程可追溯性、不变性在一定程度上仅仅解决了部分问题,商业秘密整体的安全性、稳定性保障目前依然是区块链技术保护商业秘密亟需关注解决的主要难题。

(一)公有链、联盟链、私有链保护商业秘密均存在不同程度风险

当前区块链有公有链、私有链、联盟链之分。公有链具有无国界、数据透明化、完全匿名化等典型特点,实现了完全去中心化,这也使得公有链技术保护商业秘密的风险呈现得最为突出。风险之一是,公有链的链上所有节点访问权限、记账权限及其他相关权

限完全一致，链上数据透明，信息保密难以实现；同时，一旦发生不合规、不合法利用区块链技术而需要追究责任人时，因为所有节点匿名化特质及无国界限制特质，即使依据全程可追溯性特质可以追溯到相关节点，但是由于节点权属人身份信息匿名以及可能跨越国界，无法实现追究具体责任人法律责任的目的。风险之二是，虽然区块链被称为商业秘密资产自动化交易的知识产权革命即将到来，[12] 公有区块链具备了透明性和去中心化的优势，但却丧失了速度和效率的延展性要求。区块链的延展性又被称为可伸缩性或可扩展性，是对区块链技术计算处理能力的一项指标值界定标准，用于对区块链技术处理链上事务的速度与效率的考量与评价。延展性向好的标志是处理业务的高吞吐与处理速度的低延迟，而这一些恰恰是公有区块链存在的固有缺陷。在实践中，区块链技术保护版权的应用已经因为区块链的延展性不足而导致业务普及推广不畅，商业秘密一旦全面推广上链，相应的商业秘密的数据量将会呈现几何倍数增长，区块链处理效率相比传统模式滞后太多，这种延展性不足的固有缺陷极大地阻碍了区块链技术在各领域场景应用的空间及发展前景。

为更好保障区块链的链上相关必要信息的保密性及对不合规与不合法行为的可追溯性及责任认定，以“中心化系统”为代表的私有链、基于不同私有区块链之间信息互认等需要产生的联盟链成为当前区块链技术的新阶段。联盟链的开发使用被视为区块链3.0版本代表，其典型特点是延展性好，解决了以往区块链延展性不足的固有缺陷，但是目前联盟链主流仅处于1.0版本阶段，联盟链自身也面临着联盟成员联合欺诈、利益不均衡、数据资产权属不清等典型问题。私有链保护商业秘密在这三类区块链中安全系数最高，但是因为其中心化系统特征明显，与区块链去中心化及难以篡改特征相去甚远，对于数据化商业秘密的真实性、保密性、稳定性保障与传统电子数据面临同样的缺陷，难以达到真正保密目的。联盟链与私有链，因为实名绑定的身份限定及不同身份节点人的访问权限及访问内容不同，减少了数据上传量，同时也不要求所有节点都负有打包确认及存储义务，其延展性得以发挥，但这是为了实现可追溯性及延展性而牺牲了区块链固有的去中心化、公开透明特质，一旦中心化系统授权访问人不诚信或中心化系统被黑客攻击，商业秘密更容易被泄密、窃取或篡改，同时这种情形下的区块链延展性是否充分就失去了应有的价值和意义。

（二）区块链技术难以完全保证商业秘密上链前的真实性及上链后的保密性

如前所述，区块链保护商业秘密，在实践中一般采取的是权利人自行利用私有链或其他设备存储商业秘密原始资料数据，然后将商业秘密数据打包成哈希值上传联盟链或公有链，在联盟链或公有链层面看到的只是数据化商业秘密的哈希值，由于哈希值不可逆性及算法黑箱的特质，商业秘密的真实性、秘密性与保密性得以保障。但是，商业秘密的真实性、秘密性与保密性仍面临如下风险：

一是商业秘密上链前的真实性无法保证（即虚假储存）的风险。商业秘密虚假存储的风险，在《人民法院在线诉讼规则》第十八条有明确规定：一方当事人有权就电子数据上链储存前的真实性依据新证据提出异议，另一方当事人有义务就该电子数据上链前真实性提供相应证据供人民法院审查、确认。本规定恰好说明了电子数据上链前的真实性并非绝对安全，存在虚假信息存储的风险。此类风险主要体现为商业秘密权利人存储商业秘密原始资料数据所凭仗的私有链或其他设备的不安全，包括私有链密钥丢失或被窃取导致商业秘密数据泄露、私有链某个或某些节点主动泄密、私有链超过50%节点被黑客攻击篡改数据使篡改后的数据取代原商业秘密数据成为合法数据、为私有链提供数据服务的服务商在后台利用数据对后台透明的缺陷不法获取商业秘密、其他设备被攻击导致商业秘密泄露或被窃取等。

二是商业秘密上链后的泄密风险。经过对商业秘密进行哈希计算后，因哈希算法单向不可逆，上传公有链或部分联盟链后无法还原为原始电子数据，因此一般不存在泄密风险，但也并非绝对。实质而言，存储与泄密风险属于区块链技术中的全链条系统性风险，并非在某一个时间段才能存在，需要多方的共享融合和技术支持。《最高人民法院关于互联网法院审理案件若干问题的规定》第十一条规定，当事人“通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存储平台认证”提交的电子数据，并非具有当然的证明效力，还需要证明其真实性，得到互联网法院

的确认之后才能发挥其应有的证据效力。《人民法院在线诉讼规则》第十五条规定,“当事人作为证据提交的电子化材料和电子数据”,也只有经人民法院依法查证属实后,才能作为认定案件事实的根据。这些规定也说明了区块链技术存储的商业秘密信息在上链后并非完全没有任何风险。如果存储平台和当事人具有利害关系、双方之间存在“联盟链”的“不正当关联”关系、恶意强行篡改链上信息,“虚假信息”都有可能成为“法律事实”,《人民法院在线诉讼规则》第十七条列举的四项情形就是针对区块链技术存储的电子数据上链后的真实性审查的标准和依据,其中就包括了因存储平台资质不合法导致的区块链技术存储信息证据力丧失的风险、当事人与区块链存储平台存在利害关系并利用技术手段不当干预证明过程的风险、存储平台存储信息技术规范标准不达标的风险等。很多商业秘密权利人在实践中一般将商业秘密数据先存储在不同的云平台,之后在云平台上将其打包成哈希值,上传区块链。这样做的最大风险是其利用的是云平台打包工具,商业秘密原始数据资料对于云平台服务商是透明的,遇到不诚信的云平台服务商或工作人员,非常容易泄密。

(三) 智能合约法律规制不健全

区块链技术保护场景下的商业秘密面临的各类风险在根本上都可以体现为智能合约(及相关)风险。智能合约与电子合同及纸质合同根本不同,智能合约不是单纯的电子合同,理论上应该是一种模式,是“计算机代码语言构成的技术类计算机共识文本+可视化电子合同或客户端电子交互模块”的结合模式。智能合约风险主要体现为三个方面:一是这种模式的底层共识文本与表层可视化客户端都可能被攻击篡改,导致风险的发生;二是即使各节点按照自动触发原则正常执行智能合约,也可能发生当事人主体真实身份确定不能、民事欺诈与刑事犯罪情节认定不能、当事人意思表示撤回与撤销不能等各类风险;三是司法程序中的区块链技术保护商业秘密被侵害事实的证明与损失鉴定问题属于新业态电子数据的证据举证质证表现形式,智能合约及相关各方当事人的权利义务界限与侵害行为认定依据现行法律可能面临无具体法律规定的情况,需要办案人员根据个案灵活把控,无形中就会出现自由裁量权、释明权的边界把握的难题。

国家互联网信息办公室 2019 年公布实施《区块链信息服务管理规定》对规范区块链信息服务活动、最高人民法院 2021 年 6 月公布实施《人民法院在线诉讼规则》对推进和规范区块链形式的在线诉讼活动及完善在线诉讼规则等作出了明确规定,但都没有涉及智能合约问题。智能合约当前在我国还不是一个法律上的概念,通常被认为是区块链应用场景中电子合同的一种特殊表现形式,更有部分学者与法律实务人士不认可智能合约的合同属性,认为智能合约当前最多属于电子合同履行的一种方式。电子合同在我国的直接法律规定是《中华人民共和国电子签名法》(以下简称《电子签名法》)、《中华人民共和国电子商务法》(以下简称《电子商务法》)及《民法典》等。《电子签名法》第三条限定了民事活动中电子签名的约定性,在婚姻、收养等人身关系和停止供水供电等公用事业服务方面也作了排除性使用的强制规定。《电子商务法》第二条和第十条规定了电子商务规范的范围是经营活动,经营者作为电子商务主体应该登记。《民法典》第四百六十九条和第五百一十二条分别规定了电子合同的形式及电子合同因标的不同而交付时间不同。

上述法律制度中的电子合同及电子签名均是由民事主体在法律允许的范围内自行完成的,其典型特征是主体身份的特定性与明示性、适用领域及范围的有限性、合约履行的线上约定与线下验证相互印证性等。智能合约作为区块链场景应用下的自动触发形式的履行模式,代码是其基础表现形式,可视化客户端只是其执行程序。智能合约代码的撰写方可能是合同当事人之外的第三人,第三人撰写的智能合约代码内容是否能够真实表示合约当事人的意思,是否能够在区块链应用场景中克服区块链延展性不足的缺陷,确保合约履行符合当事人的预期等问题,都还是处于不确定的状态。第三方起草的代码是否能够真实表示当事人的意思,不仅仅取决于代码撰写方的主观理解能力,还可能与代码的客观表达形式及表达效果有关系。代码为核心的智能合约如果履行延迟甚至失败,也许与代码撰写方客观能力有关系,但更为重要的是来自区块链技术延展性差的客观缺陷。智能合约不同于一般的电子合同,区块链技术应用中的分布式节点与匿名性特征,决定了合约主体自始至终的不确定性,一旦出现合同欺诈,责任人无法追溯和

确定。对智能合约如何准确规制，在上面所述的三部法律中都未有对应性措施。在区块链技术应用过程中，智能合约现实使用与民事合同规制也存在严重的法律错位问题。

四、实践调研：“区块链+商业秘密”模式应用喜忧参半

从二十一世纪初的比特币开始的理论概念到当前的实践应用，区块链在我国短短的十几年时间里诞生了两万家左右区块链业务企业。目前，区块链业务企业大多数提供以“数据存储、取证”为核心的版权保护与电子数据存储业务，即以“区块链+版权”模式，用区块链技术将权利人的版权作品固定、展示与存证，保障权利人对作品复制、修改、传播等过程的全程透明与可追溯掌控，从而避免被侵权的风险。相比之下，“区块链+商业秘密”模式，是以区块链技术将权利人的商业秘密上链储存及依法流转，实现商业秘密保密存储及合法使用之目的，理论上虽然具有去中心化、难篡改、以哈希值形式体现秘密数据、全程可溯源等天然优势，但在实践中并未能得到广泛的推广应用。这主要是因为商业秘密作为无形资产，必须依附于某种介质或载体存在，往往以书面形式或电子数据形式进行存储、使用和流转，从而决定了侵权行为的隐蔽性、私密性和非固定性，使侵权证据易于藏匿且偏在于侵权人。[13] 即使在区块链技术场景下亦是如此。为更深入地了解区块链技术保护商业秘密的社会实践状况及面临的主要问题，笔者围绕区块链技术平台对上链前后的商业秘密保密、前置性商业秘密司法鉴定等两大典型难题进行了调研。

（一）“区块链+商业秘密”模式缺乏应对隐蔽侵权行为的有效保密措施

笔者通过对杭州某科技有限公司以及北京某天平科技有限公司的调研发现，“区块链+商业秘密”模式应用存在两个典型共性问题。首先，公司的日常业务中确实有关于技术秘密的区块链上链业务，但是公司后台只负责数据的加密存储工作，没有针对相关数据的业务量及业务类型的汇总统计工作，即不介入客户技术秘密数据的实质性分析及处理。第二，网络系统的本身特征，决定了客户提交的隐私数据对于其他客户、链上交易人等主体而言，属于没有公开的秘密数据，但是对于区块链业务后台及数据库后台而言，这些数据却是透明的。如何约束平台及相关工作人员则是一个非常现实的问题。对区块链平台及其工作人员的传统约束，一方面来自职业道德的内在自我约束，另一方面来自与客户签署的保密协议的外在约束。一旦后台工作人员在加密储存过程中违规盗取了客户技术秘密数据信息，也是基于数据库后台的透明性特质而获取，属于典型的隐蔽性质的侵权行为，客户难以发现。实践中对此的普遍做法是，商业秘密涉及到公司客户的技术秘密与经营秘密，很多客户宁愿通过企业内网与公共网络之间的物理隔断来进行保密运行，也不愿冒险通过区块链进行商业秘密信息的存储。即使有的企业通过区块链平台提供了商业秘密数据信息，由于区块链平台只是媒介，并不拥有商业秘密信息处分权，也无法左右商业秘密权利人对信息的具体处置。对于如何防止二次泄密，除了上述内外约束机制，客户也可以选择在链下做好数据保密工作后将哈希值上传，这样能最大程度保障商业秘密的安全。对于如何在链下做好数据化信息的保密工作，对区块链技术平台公司而言，依然是一个现实的普遍难题。

（二）前置性“区块链+商业秘密”司法鉴定有现实需求，但难以实现商业化

前置性商业秘密司法鉴定是指所有非诉类的商业秘密鉴定，目的在于对企业日常商业秘密保护情况进行评测，提出完善方案并协助执行，防范可能性的侵害商业秘密风险。前置性商业秘密司法鉴定是企业在日常商业秘密管理过程中，对自身商业秘密的非公知性、保密性、商业价值性等所做的主动性保护行为及委托鉴定行为。鉴定内容一般包括三个方面：企业对自身商业秘密管理体系的构建、保护、发展及规划的合理性与可行性评估及实践；企业因首次公开募股、商业秘密质押融资等原因，为提高无形资产价值而对企业商业秘密做的鉴定；企业在发觉员工有违反保密协议、保密制度或竞业限制协议的意图或动机时，在行政执法、司法程序启动前所采取的主动性商业秘密鉴定。通过权威机构出具的商业秘密鉴定意见，在对员工起到制止和警示作用的同时，企业也能够使自身的商业秘密得以更好的保护。

鉴于区块链技术保护知识产权的天然优势，目前，前置性“区块链+商业秘密”等知识产权类司法鉴定已有诸多实践案例。笔者对山东省某计算机司法

鉴定所就区块链等电子数据前置性司法鉴定调研时发现,部分企业通过这种前置性司法鉴定获得了商业秘密等知识产权的第三方证明,一旦未来发生纠纷,权利人可以将其用作纠纷争议解决的证据使用。但是,这种模式当前并未实际大规模开展,因为涉及到收费问题,企业不愿意为尚未发生争议的知识产权鉴定买单,司法鉴定机构难以在此业务中实现盈利。该司法鉴定所的已有知识产权前置性鉴定大都以免费为主,支撑该鉴定机构此类业务的主要是政府财政资金或科研项目资金,与商业化应用尚有较大距离。

五、解决思路:强化对区块链、人工智能算法、智能合约等电子数据相关问题的法律规制

立法的完善与执法的严格落地是我国当前商业秘密保护的重点工作和发展趋势。要从根本上解决商业秘密的存证问题,应更多地关注商业秘密保护的技术问题。在探讨制定统一的《商业秘密法》或继续完善《反不正当竞争法》的同时,新兴和逐步完善的区块链技术未尝不是商业秘密管理和保护更为便捷可行的一条路径。针对上述典型问题,区块链技术保护商业秘密的完善可以考虑从以下几方面展开:

(一)完善“跨链兼容”模式,推广“前置性电子数据鉴定”商业化业务

当前我国区块链技术已广泛应用于数字金融、物联网、智能制造、供应链管理、数字资产交易等各个领域,随着社会上大数据、云计算、网络化的快速发展,各行业、各领域商业秘密数据化保护进程将会不断加快,区块链是截至目前应用前景最为广阔的保护商业秘密的一项技术集成模式。如前文所述,公有链的所有链上数据的公开透明特质并不适合商业秘密保护,只有“应用层的公有链+扩展层的联盟链+底层的私有链”融合模式才是对商业秘密保护相对最优的选择。商业秘密原始数据信息存储在私有链、联盟链甚至是权利人自己的设备中,公有链显示的只是打包后上传的哈希值,它可以很好地保证商业秘密的真实性、秘密性。实践中,通常情况下是在区块链底层技术结构基础上实行公有链、联盟链、私有链相结合的分层运行机制。私有链以私钥为入链依据,联盟链各链之间设置访问限制、浏览限制等不同权限,如此,可很好地保障链上数据信息的安全,并能因其实行的身份绑定的特征实现身份溯源及责任追究的目的。基于此,区块链技术保护商业秘密以“私有链(或在联盟链)为原始信息存储地+公有链(或在部分联盟链)上传哈希值”的“跨链兼容”模式为典型表现形式。“跨链兼容”模式主要指的是“标准共识兼容插件+多链并存与跨链兼容”。本模式主要解决两个问题:第一,为实现区块链真正的可全程溯源目标,将区块链访问端口与访问者的身份实现绑定,以实名制加强区块链法律规制;第二,为避免公有链全程透明与商业秘密保护冲突的问题,将公有链、联盟链、私有链分别设置在系统的应用层、扩展层和底层。应用层进行哈希值展示、扩展层对商业秘密原始数据进行有限访问、底层对商业秘密原始数据的数据存储分层控制。这一模式的正常运行,需要某一应用领域的政府或其授权方主导的区块链服务管理方,设置统一的标准共识算法,将其体现为类似于 U 盘的可插拔插件载体(或其他链接程序软件等形式),供其他合法的区块链服务商跨链融入,以此实现各链所存储商业秘密信息的互认与依法使用。

在当前法律体制下,普通区块链企业并不相当然具有电子数据存证资质,其数据秘密信息的真实性不能作为直接的判案证据使用,一旦纠纷发生,当事人只能重新申请有资质的鉴定机构重新鉴定。区块链技术存证本身是对商业秘密的一种证明行为,重新申请鉴定的过程就成为了二次证明,导致证据资源的重复浪费和诉讼效率的低下。因此,对于符合《区块链信息服务管理规定》要求的区块链服务企业,应扩大他们参与司法证据存证等业务的机会。可以采取“标准共识兼容插件+多链并存与跨链兼容”模式,既能保证各链机会均等地争取商业秘密数据存储的机会,更能保证一旦发生纠纷时,电子数据证据来源能够多元,使得司法过程中的举证与质证机会公平。而实现这一目标的基本前提,则需要最高人民法院的司法区块链平台、金融区块链管理平台、医疗系统区块链管理平台以及物联网区块链管理平台等面向普通区块链企业开放“标准共识插件”接入的机会。随着数字化社会的快速发展,包括商业秘密在内的各类信息上链将在各领域成为常态。

由于区块链企业的良莠不齐,强化对区块链技术保护商业秘密企业的资质审查、行业诚信意识与氛围的培养,将成为一项基础性的必要工作。为此,应该鼓励区块链服务商及电子数据类司法鉴定机构等单

位，协同为企业等商业秘密及其他类型电子数据权利人提供前置性数据上链等风险规避服务，在此基础上将其与行政执法及司法过程中的电子数据证据存证、举证等程序相衔接，增强企业常规保密意识、保密能力与电子数据类证据存证、举证与质证的能力，改变当前我国商业秘密领域内取证难、举证难、质证难以及因此造成的成案率低、胜诉率低的顽疾。根据笔者对山东某电子数据司法鉴定所的调研情况显示，该鉴定所已经应企业请求，由法定的知识产权司法鉴定机构联合区块链企业共同完成了数例商业秘密与其他电子数据的前置性上链认证工作。如此，一旦发生纠纷，上述相应基础性的前置性证据上链存证工作将作为有效的证据提交给裁判机关，有效避免了当前商业秘密纠纷案件中举证质证难的问题，这种做法值得在司法实务中广泛推广。而前置性知识产权司法鉴定业务谁来买单这一现实问题也需要综合考量。一方面需要鉴定方或区块链服务方不断提高和完善存证能力，为企业提供更好、更高价值的服务，吸引企业主动为他们的服务买单；另一方面需要国家主管单位加强宣传，提高企业加强商业秘密保护的意识，才能推动企业与前置性商业秘密司法鉴定与上链存证业务对接及可持续推进。

（二）完善区块链诉讼证据提交与审查机制

依据《中华人民共和国民事诉讼法》第六十三条规定，电子数据属于八大类民事诉讼证据之一。与其他电子数据一样，诉讼中使用的区块链证据仍需经过举证和质证程序，接受人民法院对证据“合法性、关联性、真实性”的“三性”审查，而不能仅仅因为某一电子证据是区块证据就认为其效力是万无一失。[14] 区块链技术并不能提供绝对意义上的反篡改，区块链电子证据的反篡改具有相对性。[15] 加强对提交的区块链诉讼证据的审查至关重要。

区块链技术保护商业秘密过程中发生的侵害方式与传统侵害有本质不同，最典型的是对“以盗窃等不正当手段侵害区块链技术保护商业秘密”方式的理解与取证应用。根据《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（三）》第三条规定，《中华人民共和国刑法》第二百一十九条第一款第一项规定的以“盗窃”或“其他不正当手段”侵害商业秘密，主要表现为“采取非法复制、未经授权或者超越授权使用计算机信息系统等方式窃取商业秘密”与“以贿赂、欺诈、电子侵入等方式获取权利人的商业秘密”，这也是诉讼过程中举证质证的重点。作为受害方的区块链技术保护下的商业秘密权利人的认定也和传统领域不同。2020年9月实施的《最高人民检察院、公安部关于修改侵犯商业秘密刑事案件立案追诉标准的决定》将商业秘密刑事案件追诉一般标准降为三十万元，其中第一个标准是“给商业秘密权利人造成损失数额在三十万元以上”。这里的“商业秘密权利人”在传统刑事案件中可能表现为单一主体，而在区块链刑事案件中则可能是多个节点主体组成的整体。如以太坊上一个众筹Dapp（去中心化应用）的“The DAO”系统漏洞被黑客利用，直接导致了价值6000万美元的数字货币被攻击者窃取。该案受害的权利人来自区块链上智能合约的众多节点，单一受害人可能受损失数额不大，但是众多区块链节点的受害人叠加的损失数额巨大，这也是区块链案件的典型表现。因此，司法实践中，应以一个受害整体的损失数额作为刑事责任起刑点认定标准。

区块链技术保护下的商业秘密一旦受到侵害，由于网络数据的虚拟性与可跨境性特质，对侵害方的确定与责任追究呈现出难度大、复杂程度高、取证难的典型特点，因此，加强对电子数据类证据的认定标准的规范至关重要。根据2020年5月1日最高人民法院实施的《关于民事诉讼证据的若干规定》第十四条、第十五条、第九十条、第九十三条、第九十四条的规定，电子数据也必须符合证据“三性”标准，有疑点的电子数据不能单独作为认定事实的依据，认定电子数据真实性有五类直接认定标准与七类审核性标准。区块链属于其中所谓的“其他以数字化形式存储、处理、传输的能够证明案件事实的信息”的证据形式，当事人提交的电子数据形式的证据一般应该是原件或电子数据的制作者制作的与原件一致的副本、或者直接来源于电子数据的打印件或其他可以显示、识别的输出介质等可被视为电子数据原件的形式。区块链证据多以“可显示、识别的输出介质”为主，对“可显示、识别”的证据力把握成为区块链证据提交与审查的重点。当事人提交的区块链证据如果无法实现“可显示、识别”功能，而对案件裁判又至关重要的情况下，对区块链等电子数据的司法鉴定可作为区块链证据提交与审查的补强措施。根据《关于民事诉讼

证据的若干规定》第九十三条及《关于知识产权民事诉讼证据的若干规定》第十九条的规定,对于“电子数据的真实性、完整性”等待证事实,人民法院可以将其中的专门性问题委托鉴定或勘验。由于当前我国知识产权鉴定机构及其司法鉴定业务已被 2020 年 4 月 1 日实施的《司法部办公厅关于开展司法鉴定机构和鉴定人清理整顿工作的通知》的规定排除在外,公检法各单位没有统一的知识产权司法鉴定名册,实践中容易发生不同阶段的知识产权司法鉴定的鉴定意见相互矛盾与冲突的现象。因此,行政执法与司法各阶段的办案人员在委托鉴定时应当尽可能以行业内公认的权威鉴定机构作为委托对象,以保证鉴定意见的权威性与证据效力,也保证各阶段对司法鉴定认知的一致性,从而提高办案效率与公正。

(三)完善对智能合约的法律规制

法律规制的基础,是在认识智能合约风险基础上,全面了解智能合约的缺陷与不足。《民法典》第四百六十九条规定的“以电子数据交换、电子邮件等方式能够有形地表现所载内容并可以随时调取查用的数据电文”订立的合同,我们将其称为电子合同。智能合约与电子合同、纸质合同在属性方面有本质不同。如前所述,智能合约的端口可视化应用表现形式一般是电子合同的形式,除此之外还有作为代码形式出现的技术层作为合约执行的基础支撑。智能合约不等同于具有法律效力的合同,认定其效力应结合智能合约应用中的具体问题展开具体分析。[16] 由于智能合约“合约+执行”的不可逆特性,相比传统合同而言,当事人一般不存在违约的机会,当然也不存在救济的可行性。[17] 一旦有违约情况发生,虽然在国际商事领域中适用智能合约具有提高交易效率的速度优势,但是智能合约的自动执行性使得当事人的违约成本大大提高。[18] 换言之,智能合约具有明显的效率优势,但由于智能合约的订立是以写入计算机代码形式完成,存在无法完整表达当事人意思的缺陷[16]。智能合约这种不可逆转的自动性和执行性容易使它极易成为犯罪行为的完美载体。犯罪分子可以完美利用区块链智能合约的无第三方中立机构以及自动触发执行的特性,将犯罪信息输入并将法定货币转换为数字货币汇入区块链虚拟托管账户而完成委托。智能合约匿名保护等特质使得非法活动更难被执法部门监控,即使案发也很难被侦破,所以其社会危害性范围会更加广泛,危害会更深。[19]

面对智能合约来自于计算机代码与算法撰写人的主观倾向及客观网络治理的缺陷,国家立法与执法层面应致力于将法律与代码、算法深度融合,强化对代码、算法等计算机语言的依法治理与全面规范,关键是强化对智能合约主体的可识别性法律规制。改变智能合约关系的主体匿名性、保证智能合约的真实主体可识别性是法律规制的基础,这也是强化智能合约的现实可执行性的基本要求。要保证智能合约内容能够完整表达当事人的意思表示,并在各节点被普遍理解,这是当前以计算机代码形式所代表的智能合约内容最大的局限及今后努力方向。后续智能合约相关立法应该在保障智能合约可视化内容与订约人真实意思表示之间的一致性方面不断探索并加强立法规制,保证智能合约关系如现实合同关系一样容易理解并真正执行。这需要在公有链的基础上强化联盟链应用能力的法律规制,或有其他能够有效识别各节点主体身份的法律规制措施。只有智能合约主体真实身份可识别,才能有效减少智能合约底层共识文本与表层可视化客户端被攻击篡改的风险、避免智能合约因自动执行导致民事诈骗无法追究具体的责任人风险。对于智能合约自动触发及履行的特性,合约关系真实身份的确定也有助于当事人依法对合约的变更、撤回、撤销等行为的正常执行。

综上所述,商业秘密作为所有企业最重要的核心资产,对企业合法权益维护、企业正常存续发展及国家的市场竞争秩序的公平与稳定影响巨大,我们应在借鉴发达国家先进理念的基础上结合我国的具体情况加大保护力度。从实践来看,区块链技术保护商业秘密作为知识产权数据化的典型代表,是当前相对最优的模式选择,具有广阔的应用空间和发展价值。美国佛蒙特州、伊利诺伊州等相继出台实施区块链技术法案、区块链合同法案等,对智能合约进行了法律肯定,但也在认可区块链难以篡改的基础上认为其依然具有被篡改的可能性,无法从根本保证上链证据的绝对真实及上链信息的绝对安全。美国作为商业秘密保护最完善的国家,依然在区块链技术保护商业秘密问题上难以形成有效规制,说明了区块链技术保护商业秘密等电子数据类知识产权的复杂性。用身份认证绑定区块链应用场景以加强商业秘密保护,强化公有链、联盟链与私有链的分层融合与跨链兼容平台保

障商业秘密数据真实与安全，完善对智能合约的法律规制是应对上述问题的主要法治策略。这对于解决区块链追溯真正的责任主体难、区块链应用的实践延展性不充分等现实难题意义重大。从商业秘密风险预防及区块链全程可追溯的电子证据存证优势角度来看，在区块链技术应用场景中鼓励企业等市场主体积极开展前置性商业秘密司法鉴定，规范布局区块链技术存储商业秘密业务，对于提升权利人的商业秘密举证能力、从根本上防范商业秘密风险及提高商业秘密案件的成案率与胜诉率具有积极意义。

参考文献：

[1] 唐青林，黄民欣主编.商业秘密保护实务精解与百案评析[M].北京：中国法制出版社，2011.

[2] 杨帆.大数据时代下数字版权与信息自由的冲突及协调[J].理论观察，2021，6.

[3] Heo，Gabin，et al. Design of blockchain system for protection of personal information in digital content trading environment [J]. International Conference on Information Networking (ICOIN). IEEE，2020.

[4] 吴为.区块链实战[M].北京：清华大学出版社，2017.

[5] [日]野口悠纪雄.区块链革命：分布式自律型社会出现[M]，上海：东方出版社，2018.

[6] [美]斯延森.密码学：理论与实践[M].北京：电子工业出版社，2009.

[7] 张怀印.区块链技术与数字环境下的商业秘密保护[J].电子知识产权，2019，3.

[8] 李晓辉.算法商业秘密与算法正义[J].比较法研究，2021，3.

[9] Singh，Kalpana，et al. A Novel Credential Protocol for Protecting Personal Attributes in Blockchain [J].Computers & Electrical Engineering，2020，83.

[10] Holbrook，Joseph.Architecting Enterprise Blockchain Solutions [M]. John Wiley & Sons，2020.

[11] Gurkaynak，Gonen，et al. Intellectual Property Law and Practice in the Blockchain Realm [J].Computer Law & Security Review?，2018，34.

[12] Halligan R M. Automated Trade Secret Asset Management：SFP Classification，EONA Proofs，Blockchaining，and DTSA Civil Seizure Orders [J]. UIC Rev. Intell. Prop. L.，2020，20.

[13] 潘剑锋，牛正浩.书证提出命令程序性制裁理论检视——以商业秘密侵权诉讼为切入[J].政法论丛，2021，5.

[14] 蒋鸿铭，吴平平.《人民法院在线诉讼规则》区块链证据规则若干问题探析[J].法律适用，2021，7.

[15] 龚善要.论区块链电子证据的双阶鉴真[J].西安交通大学学报(社会科学版)，2021，1.

[16] 郎芳.区块链技术下智能合约之于合同的新诠释[J].重庆大学学报(社会科学版)，2021，5.

[17] 李旭东，马淞元.《民法典》合同编视域下的区块链智能合约研究[J].上海师范大学学报(哲学社会科学版)，2020，5.

[18] 孙雯，范玉颖.CISG下智能合约的适用问题研究——区块链技术的法律限界[J].商业研究，2020，10.

[19] 赵志华.区块链技术驱动下智能合约犯罪研究[J].中国刑事法杂志，2019，4.

Application and Legal Regulation of Blockchain Technology in Trade Secret Protection

Xing Yuxia[1]，*Song Shiyong*[2]

(1.Civil and Commercial Law School of Shandong University of Political Science and Law，Jinan Shandong 250014；2.Political Science and Law of Qilu University of Technology (Shandong Academy of Sciences)，Jinan Shandong 250353)

【Abstract】With the rapid development of big data and artificial intelligence algorithms，blockchain technology has shown outstanding advantages in protecting the authenticity of trade secret data，but it also faces various risks，such as systematic risks in the form of public chain and alliance chain，insufficient realization of the extensibility value of blockchain itself，and imperfect high-level legal regulation of blockchain. Exploring the mode of "standard consensus compatible plug-in + multi-chain coexistence and cross-chain compatibility"，encouraging pre-judicial authentication of trade secrets，improving the evidence mechanism of blockchain litigation，and strengthening the legal regulation of smart contracts have become the necessary choices for blockchain technology to protect trade secrets.

【Key words】trade secrets；blockchain；smart contract；access to evidence；pre-judicial authentication

(责任编辑：唐艳秋)