论区块链存证电子数据的优势及司法审查路径

石冠彬　陈全真

[提要] 基于电子数据易于篡改或伪造的特性，电子数据的真实性判定始终是证据法理论难以突破的瓶颈，导致司法实务对电子数据的采信率极低。区块链技术通过“司法联盟链”的构建，能确保电子数据在产生、收集、保存、传送的各阶段不被篡改或伪造，从而较好地解决其真实性认定问题，并且经区块链存证的电子数据可无障碍地认定为证据原件。现行互联网法院的司法实践，先于立法对通过区块链技术保存的电子数据效力予以广泛认可，值得肯定。未来理论与实务应当致力于在技术层面进一步构建区块链存证电子数据的运行机制，实现区块链技术融入证据法理论之中，并总结司法实务有益经验致力于构建一套适用于区块链存证电子数据的审查认定规则，并配置相关制度解决电子数据在形成之初可能出现的伪造问题，促使该新技术手段彻底解决电子数据的真实性认定难题。

[关键词] 电子数据；区块链技术；区块链存证；真实性；证据原件

中图分类号：DF713　　文献标识码：A　　文章编号：1004—3926（2021）01—0067—07

基金项目：国家社会科学基金重大项目“健全以公平为原则的产权保护制度研究”（20ZDA049）、国家社科基金重大项目“中国特色自由贸易港的建设路径及法治保障研究”（18ZDA156）阶段性成果。

作者简介：石冠彬，甘肃政法大学特聘教授，海南大学法学院教授、博士生导师，研究方向：民商法学。甘肃 兰州 730070　陈全真，南京大学法学院博士研究生，研究方向：民商法学。江苏 南京 210023

自杭州互联网法院2018年6月28日首次确认采用区块链技术存证的电子数据具有法律效力①以来，区块链存证电子数据已经逐步为互联网法院所认可：一方面，最高人民法院2018年9月7日发布《关于互联网法院审理案件若干问题的规定》，该司法解释第11条第2款明确通过区块链技术存证的电子数据如果被认定为真实，可作为有效证据采纳，从而使得区块链存证在司法适用中得到了实质层面的推进；另一方面，互联网法院的司法实践极大地推进了区块链存证技术的应用，自杭州互联网法院2018年9月上线全国首个司法区块链平台以来，北京互联网法院主导建立了司法区块链——“天平链”，根据2019年9月3日发布的《北京互联网法院审判白皮书（2018.9－2019.9）》显示，“天平链”目前完成跨链接入区块链节点18个，上链电子数据超过696万条，跨链存证数据量已达上千万条，在实际审理的案件中已经验证跨链存证数据1301条。那么，究竟应当如何认识区块链技术在电子数据存证上的优势？对此，本文将在考察区块链存证技术应用背景的基础上，就区块链存证技术如何保障电子数据不被篡改进行分析，并就该类电子数据在证据属性上属于原件进行论证，最后讨论应当如何构建此类电子数据的“证据三性”审查规则。

一、区块链存证技术运用的背景：源于电子数据的真实性难以认定的实务困境

（一）电子数据司法适用的现状：采信率极低

随着互联网信息技术的高速发展，电子数据作为证据材料在法庭上出现的频率越来越高，我国现行《民事诉讼法》（2017年版）第63条第（五）项、现行《刑事诉讼法》（2018年版）第50条第（八）项、现行《行政诉讼法》第33条（2015年版）第（四）项均明确将“电子数据”作为法定的证据类型。与此同时，从司法实务来看，电子数据的司法适用存在相当的困境，相关难题围绕电子数据的真实性认定展开。有学者曾以中国裁判文书网2012年之后的“民事案件”为样本，以“电子数据”和“电子证据”作为关键词进行检索，分别获得4777个和15541个案例，这些案件清晰地反映了电子数据的司法适用困境。[1] 具体而言，电子数据在司法

实务的采信情况主要表现为如下两方面:

一方面,电子数据的采信率极低。有学者曾在文章中指出,电子数据在司法实务中的采信率仅占总数的 10% 左右。[2] 杭州互联网法院副院长官家辉 2019 年在浙江卫视《今日评说》栏目中表示,有一个针对法院 2 万份判决书的大数据分析结果显示,法院对于电子数据的正面采信率仅 7% 左右。显然,电子数据在司法实践中的采信率是无法做准确统计的,但是不同样本的分析结果至少表明,电子数据的采信率确实极低。分析部分判例,可以发现法院不予采信电子数据,主要是基于无法对电子数据的真实性作出全面准确鉴别的原因,其表现形式要么是无法证明电子数据的客观真实性或完整性,②要么是电子数据的上传时间无法证明……真实性与关联性均无法确认等。③

另一方面,即使是能够得到采纳的电子数据,司法机关中也有法院将其转化为物证、书证或言词类证据加以采用,[3] 这种裁判的做法就使得作为法定证据种类的电子数据形同虚设。简言之,仅由于基层法院技术鉴定能力有限而将电子数据转化为传统的证据种类,这种虚置化的应用实质上是否定了电子数据这一独立的证据种类,是对证据法体系的反噬。由此可知,在司法实践中,电子数据的鉴别难度较高,对其司法适用提出了非常高的要求,并由此产生了电子数据证明力低下的现实问题,并导致电子数据的采信率极低。

(二)电子数据司法适用出现困境的原因分析

电子数据司法适用困境的出现,其根本原因在于电子数据真实性的认定障碍,大致可概括为如下两方面原因:

一方面,电子数据内容的真实性、完整性和电子数据产生到传送的整个过程对于其真实性认定具有至关重要的作用。尤其是数据的保存和传送过程,该过程高度依赖于互联网、计算机等通信设施,且篡改或伪造一般不会留下痕迹,法官作为非专业人士一般无法察觉电子数据是否被篡改或伪造,在采用与不采用之间也只能依靠自由心证作出选择。因为电子数据实质上是以 0 和 1 或 on 和 off 来表达信息的二进制电磁代码,在诉讼程序之外是一种以数据为存在基础的、无体性的证据材料,其具有的电子化特征决定了电子数据是极其脆弱的,这就决定了电子数据不会像传统证据那样易于保存和固定。具体而言,电子数据不但极易被篡改或伪造,而且其收集和传送过程极易受到电磁信号干扰;当存储设备系统发生崩溃、故障以及遭遇黑客攻击或者计算机病毒,电子数据可能会发生异变甚至灭失[4];此外,司法实务针对电子数据产生时间的判定也经常出现困扰。

另一方面,司法实务采信电子证据除了面对其容易被篡改这一特点的同时,还面临证据原件理论的重大挑战。诚如前述,电子数据容易被篡改,而电子数据一般又不存在原件与复制件的区分问题,这就使得法院采信电子数据时更需要确认举证方所出具的是原件。具体而言,“证据以收集原件为原则、复印件为例外”是证据法理论以及我国三大诉讼法所一贯秉持的立场,最高人民法院在相关司法解释中也都对电子证据的原件问题作出了特别规定。④但是,电子数据又不像传统证据一样具有原件和复制件的划分,负有举证责任的一方一般很难说明哪些数据更原始,不论是通过打印、拍照等方式将电子证据出示给法庭,还是直接提交电子证据,一旦另一方对电子数据的真实性、完整性提出质疑,而负担举证责任的一方却无法证明自己所提交的证据是最为原始的电子数据时,考虑到电子数据易于篡改的特征,法官就会倾向于根据“原件标准”否定电子数据的证明力。事实上,背后深层次的原因在于“原件标准”无法回应电子数据与传统证据种类的差异。

概言之,随着科技的高速发展,通常依附于科技产品而存在的电子数据,取证、保存难度进一步加大,以至于当事人在费尽周折掌握了相关电子数据的情况下,依然因为电子数据的证明力较低而承担败诉的后果。[5] 应该说,电子数据的司法实务困境主要在于其对国家公信力的高度依赖,其根源于司法机关的技术鉴定能力不足,法官是法律的专家,但无法及时洞悉高速发展的科学技术,对于相关科技产品在司法领域中的运用准备不足,这在一定程度上也削弱了电子数据的运用效率。或者说,电子数据的无体性决定了其鉴真难度远高于普通证据种类,法官对于此种无体性证据的真实性持相当谨慎的态度。

二、区块链存证技术保障电子数据不被篡改的技术原理与路径分析

(一)区块链技术的特征及电子数据存证的可行性

自 2008 年比特币进入互联网领域,区块链就开始成为新兴互联网科技的代名词。一般认为,“区块链是一种由多方共同维护,使用密码学保证

传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术。”换言之，区块链实质上是集体维护数据库的一个技术方案，该技术方案允许系统中的多个节点将某个时间段内产生的数据信息，以同态加密算法并加盖时间戳的方式记录在一个数据区块中，该数据区块密钥可以验证下一个以同样方式产生的数据区块是否真实。这样，系统上的所有节点就可以共同认定整个区块链上的数据记录是否真实。事实上，区块链以时间戳和密码学技术为依托，也就同时具有了时间戳和加密算法的多重特征，时间戳可以记录数据区块内数据生成、传送的时间，作为数据信息的存在证明，加密算法可以对数据信息进行加密，有助于数据信息的不可篡改和伪造，从而使区块链技术完美应用于公证等领域。[6] 然而，区块链技术作为多项技术整合的产物也具有自身的特性：第一，去中心化（分布式记录），即整个互联网信息系统没有中心管理机构，每个节点的权利义务均等，且任一节点发生故障均不影响整个系统的正常运行；第二，去信任化（信息公开化），即整个系统的运行规则公开透明，相邻节点之间可互相发送、读取、传播数据信息[7]，通过各个节点的独立性设置，从而保证交换的数据信息为真实；第三，通过区块链记载的信息可以说具有不可篡改性，其包括时间上的不可篡改（已发生的历史数据不可更改）和空间上的不可篡改（任一节点的数据信息版本相同），在区块链技术的运用之中，更改节点上的数据信息一般没有意义，除非更改半数以上的节点，但是控制这么多数量的节点可能性较小；第四，匿名性，即节点之间遵循固定算法，不需要公开身份即可建立信任，节点之间的隐私不会泄露。[8](P.51)

基于区块链技术的上述特性，电子数据存证可以完美应用于司法过程。在电子数据进入法庭质证程序之前，一般要经历多个主体之间的转移，比如原始存储介质中的生成和收集阶段、电子认证机构和公证处的固定保存以及司法鉴定中心和法院的传送阶段等。这些主体可以被视为区块链上的一个个节点，即从电子数据的产生到传送过程中，上述主体可以被视为整个司法联盟链的节点。用户应当首先在区块链存证系统进行注册，当通过实名认证，用户必须将公共密钥交由第三方保管，该第三方必须是合法注册且具有电子认证服务资质，实践中一般为 CA 认证中心。当认证中心登记并签发电子印鉴证明后，用户需要制作一个电子签名。该电子签名的制作必须符合《电子签名法》规定，并且可用于识别签名人身份。最终，将附有电子签名的电子数据上传至司法联盟链的系统。其后就不再需要人为操作，自动化运行的联盟链可以使所有节点，包括公证处、电子认证机构、司法鉴定中心以及法院等即时共享联盟链上的电子数据信息。

（二）区块链存证电子数据的客观真实性考察

区块链作为一项新兴的互联网技术，其最具法律价值之处就在于它为法学理论和司法实务界引入了一种有别于传统电子数据审查认定模式的“技术自证”模式。正如有论者所言，在不久的将来，所有涉及保真、验证、记录以及鉴定的领域，包括司法裁判过程中的证据保存、提交和验证，都可以借助区块链技术来完成。[9] 因为基于区块链存证的电子数据不需要像传统证据那样形成完整的证据链条，它可以基于区块链“技术自证”的效果完成电子数据的真实性检验。这种“自证式”的检验存在于电子数据从上传至司法联盟链到诉讼活动结束的整个周期内，在这个周期内电子数据不会被篡改、伪造。那么，区块链存证电子数据的运行机制究竟是怎样的，该运行机制又何以保持电子数据的客观真实性？鉴于司法实践中重点关注的是电子数据的产生、收集、保存和传送过程，本文试从这几部分来加以简要阐释：

1. 电子数据的产生和收集过程

电子数据在产生阶段的真实性，是保证其后续传递过程具有客观真实性的前提。简单地说，电子数据在生成阶段具有客观真实性要求电子数据的产生源头必须真实，即存储介质必须唯一确定，只有存储介质唯一确定，才能保证其他节点所同步更新的电子数据也是唯一确定的。诚如有论者所言，电子数据的真实性认定必须首先满足硬件载体的真实性，即电子数据的存储介质在诉讼活动中应保持原始性、同一性，不存在更换或者破坏的可能。[10] 也就是说，由于电子数据的无体性以及对存储介质的高度依赖性，要想清晰感知、理解和运用电子数据，其产生、收集就必须借助于存储介质。因此，在电子数据的产生和收集过程中，影响其真实性的因素无非就是硬件设备毁坏、故障以及遭遇黑客攻击或病毒入侵等，一旦发生上述情况，电子数据可能永久性丢失，这也是传统存证机构的缺陷。而在区块链技术的运用之中，司法

联盟链上任一节点的存储设备故障或损坏,并不会影响其他节点的数据更改、丢失,比如公证处的存储问题不会影响法院的存储状况,从而在电子数据的产生阶段就保证了其真实性。

电子数据收集同样强调数据的真实性和完整性,但数据收集时依然可能存在因存储设备维护不到位,而遭遇黑客攻击、病毒入侵以及设备损坏等问题,另外数据收集人员在着手收集数据时无法完全排除自身的主观恣意。具体而言,尽管目前的行业协会颁布了相关的行业规范,但电子数据存证无非就是两种方式:一是电子数据备份保存,二是依托于有资质的第三方存证机构进行电子数据的存证。但是,这些传统的存证方式都是将数据信息存储在硬件设备上,不排除会遭遇外部因素而导致数据灭失,并且机构内部人员对数据的篡改或伪造更是防不胜防,这也是目前绝大多数中心化机构存在的问题之一。与传统电子数据的收集过程不同,区块链存证下的电子数据收集过程是提前经用户认可并附有当事人合法的电子签名,从而同时解决上述两个问题,既通过识别出是当事人本人的操作来保证数据的真实有效,也能基于联盟链去中心化的特性而排除收集人员主观因素以及第三方存证机构篡改数据的风险。

2. 电子数据的保存和传送过程

与传统的实物类证据不同,电子数据从产生到最终进入庭审质证,中间经历多个主体的转移、传送,在这一过程中存在着电子数据的生成时间以及生成内容被篡改和伪造的可能性。实践中常见的情形是,侵权人将储存在自己设备中的电子数据篡改或伪造,导致被侵权人无法举证。证据法理论为防止证据的真实性降低,保障其进入庭审程序后经得起质证的检验,要求证据在转移过程中应当形成完整的证据保管链条。然而目前的电子数据传送过程,无法保证传送链条的完整性,电子数据在传送过程中篡改的可能性非常高,司法机关也就有可能因为电子数据的真实性降低而拒绝采纳,[11] 进而导致其无法做出正确裁判。

但是,区块链技术可有效解决上述问题,其是包括时间戳、加密算法等在内的多项技术的整合,其至少有两种途径解决前述电子数据存证的问题:第一,对电子数据进行加密,从而大大降低数据伪造或篡改的可能;第二,利用数学上的散列函数,将电子数据类型、内容以及生成时间等进行线性处理,计算出该散列函数的哈希值,通过对比链上与链下的两个哈希值来检验电子数据有无篡改。当一个文件被线性处理后,数据在那一刻就被固定了[12],一旦发生争议,将已上传的哈希值同未上传的哈希值做对比,若前后两个哈希值一致,则说明电子数据未经篡改,反之则被篡改。由此可以看出,区块链系统的运行和维护都不再依赖于数据平台,而是链上的每个节点共同参与运行维护,这也是其与中心化网络体系的核心区别。因电子数据的整个生命周期一直严格遵循区块链存证系统的运行机制,全流程未有篡改的余地,可以真正在技术层面提高电子数据的证据效力。

三、区块链存证技术所保存的电子数据属于证据原件的解释路径

诚如前述,区块链存证技术在证据法理论层面,需要回答其所存证的电子数据究竟属于原件还是复制件这一问题,在前述杭州互联网法院认可区块链存证电子数据法律效力的案件中,理论上必须解决的问题就是区块链存证的电子数据是否属于证据原件。实际上,电子数据到底是原件还是复制件以及二者的区分标准,当前国内外学者意见并未达成一致。主流观点认为,区分电子数据的原件与复制件应取决于其物质载体的原始出处以及是否直接源于案件事实。因此有论者主张可将电子数据的原件理解为“最初生成的电子数据及其首次固定保存的存储介质”。[13] 而在区块链去中心化存储模式下,按照传统证据法理论,原件论者似乎无法解释保存于各个节点存储设备中的哪一个电子数据更原始,因为都是“首次固定保存”,或者说区块链存证的每一个节点的电子数据都是原件,会出现“复制件即原件”的状况。换言之,基于区块链去中心化的特点,每个节点保存的电子数据可以通过网络共享,从这个角度上讲,区块链存证的电子数据似乎应被认定为原件。此种逻辑推理并不存在理论障碍,但在实践中却不一定能行得通。电子数据基于自身的无体性,并不会像传统证据一样发生物理变化,计算机等存储设备之间的传送决定了电子数据的原始出处很难判断。[14] 对此,本文认为如下四种证据法理论学说可较好地论证区块链存证的电子数据在证据属性上属于原件这一结论:

其一,英美法系的“复式原件说”。该理论旨在解决同一电子数据存在多个电子文档的问题,一般适用于文书一式两份或一式多份的情形,签订合同时的“一式 N 份,每份具有同等效力”就是

典型例子。[15] 在区块链存证电子数据的情形下，当用户将电子数据上传至区块链系统时，链上的所有节点都同步更新并形成该数据的副本，而这个副本的数据内容与原始数据完全相同。这就相当于“复式原件说”中的“复式”，每个节点保存的电子数据几乎同时产生，且内容完全相同，不存在哪个节点的数据更原始的问题。由此可知，“复式原件说”可以作为电子数据原件论的理论基础。

其二，大陆法系的“原始载体说”。根据该学说，若要认定为原件，电子数据必须是最初生成的原始数据或者存储于原始介质中。举例来说，倘若某种电子数据最先固定保存于计算机硬盘中，那么该计算机硬盘作为原始存储介质应视为电子数据的原件，除此之外的任何电子数据都应视为复制件。最高人民法院相关司法解释也采纳此种观点。⑤实际上，此种观点是将电子数据的原件标准等同于录音或录像等视听资料的原件标准。不难发现，“原始载体说”与“复式原件说”具有某种相似性，二者都强调原始载体对于电子数据的原件认定具有重要意义。当原始数据上传至联盟链的某个节点，每个节点就基于点对点实时通信技术完成数据信息的共享，由于是点对点实时传送，每个节点的存储设备都可视为原始载体，不存在哪个节点设备存储的数据更为原始的问题。即便是哪个节点遭到破坏，导致该节点数据丢失，也不会产生任何影响。由此可知，“原始载体说”与“复式原件说”具有天然的一致性，其也可为区块链存证的电子数据属于原件这一论断提供理论支持。

其三，“拟制原件说”。拟制是一种常见的法律认识方法，旨在将真伪不明的事物假定为真实，以便顺利适用某一法律规则。实际上，拟制作为一种带有明显人为色彩的手段，同自然判断相对应，采用拟制方式得出的结论也具有人为色彩。因此，拟制手段在解决电子数据的原件障碍上具有独特的作用。美国证据法可谓是秉持“拟制原件说”的典型代表。《联邦证据规则》中规定：“文书或录音的原件是指该文书或录音本身，或者是录音、文书的制作者或发行者意图使其具有原件效力的复本；照片的原件包括底片以及由底片冲洗出的相片；若计算机或其他装置的存储数据可以用肉眼读出、表明能以打印物的形式准确反映原始数据的，视为原件。”由此可知，美国法上的电子数据原件范围不再局限于自然意义上的原件，而是逐步扩大至拟制意义上的原件。传统的电子数据原件强调原始出处，而拟制原件却是基于法律规定或当事人约定。由此可知，未来立法完全可以直接认定区块链存证的电子数据属于原件。

其四，“认证说”。该学说主张电子数据必须通过认证才能具有原件的证据效力，即电子数据是原件还是复制件并不是其关注的焦点，只要没有通过认证，即便是原件也不具有原件的证据效力。[16] 这里的认证是指，电子数据的制作者或收集者必须要通过身份认证，电子数据的内容以及生成时间也要通过同一性证明。[15] 认证的方式既包括自我认证，也包括第三方认证，如时间戳、哈希值校验以及电子签名等。由此可见，“认证说”并不强调电子数据原件与复制件的区分，而是回避了原件与复制件的划分难题，一定程度上化解了“电子数据复制件”的危机：一方面，区块链技术应用于电子数据存证的目的在于保障电子数据的真实完整，其自身的技术特征与运行机制并没有给原件与复制件理论留下任何解释空间，区块链存证应用系统所关注的问题并非其所存证电子数据属于原件还是复制件，而是保障电子数据的真实性和完整性，第三方存证机构都可实现上述认证方式。另一方面，该学说适应互联网新兴技术的发展，不关注电子数据是原件亦或是复制件，给区块链证据这样的新兴事物预留了理论解释空间。

四、区块链存证技术所保存的电子数据如何进行“三性”审查的规则构建

事实上，法官对证据的认定和采信，实质上就是对证据证明力强弱的评估。按照一般的审判逻辑，区块链证据的审查关键在于其是否具有证明当事人主张事实存在或不存在的证明力，而证明力的概念并不具体，其本本是一个抽象的价值定性问题，必须借助证据审查的“三性”即真实性、合法性、关联性来实现，相关司法解释就此也予以了肯定。⑥在司法实践中，对于原告提交的证据，法院会首先通过审查证据是否真实、是否合法以及是否与案件事实存在关联，以判断证据的证明力高低以及是否具有证明力。在前述区块链存证第一案中，被告就对原告提交的区块链证据提出了两方面的质疑：区块链存证平台本身的合法性（涉及到区块链存证机构资质的问题）和存证操作过程的合法性（涉及到区块链存证运行机制的问题）。⑦概言之，区块链存证的电子数据的证据资格至少应当接受真实性、合法性和关联性的检验，即举证方应同时证明区块链存证机构是否具有合法资质及其

区块链存证操作过程的真实性、合法性和关联性。事实上,司法机关借助区块链的运行机制已经将此类证据的实质审查转嫁给了公证机构或当事人,自己仅需对该电子数据进行形式审查,具体而言:

(一) 区块链存证电子数据的真实性审查

按照传统证据法理论,电子数据的真实性包括两方面,即电子数据内容是否真实以及电子数据的原始载体是否唯一确定。[10] 但基于区块链存证的电子数据的真实性审查却不应仅局限于上述两方面,原因在于区块链技术是新兴的互联网信息技术,区块链证据的审查认定规则相较于普通证据更为复杂,包括区块链存证平台的技术能力问题、存证平台或其股东与当事人有无利害关系以及原始载体的可靠性等。鉴于此,笔者认为区块链证据的真实性审查应当着重注意以下几个方面:

第一,举证方应举证证明区块链存证机构具有相应的技术能力,相应的技术能力并不是指该机构需要国务院信息产业主管部门认定其具有存证资质,只要通过国家标准时间溯源以及系统时间同步与分配,从而保证电子数据生成时间的准确性,[17] 即可认定第三方存证机构具有相当的专业技术能力。技术平台不需要国务院信息产业主管部门颁发资质证书,意味着在此科技成果专利申请程序的支持下验证其具体功能,便可实现法庭质证程序中的普适性验真效果,即无须证明承载电子数据之科技载体的可信度,仅需对科技载体之承载内容的真实性作出判断。至于区块链存证机构有无存证资质,这属于行政许可问题,目前尚无行政法规对区块链存证的行业准入设定行政许可,故区块链存证机构的资质不应作为区块链证据合法性的依据。

第二,举证方应提供产生并存储电子数据的原始载体。电子数据不同于传统的有形证据,电子数据的无体性决定了人们无法对其进行物理感知甚至判断其真实性,但存储电子数据的原始载体是有形的,人们可通过查看该存储介质的参数、状态等判断电子数据是否真实。这种审查方式和“原始载体说”的要求是一致的。第三,应借鉴杭州互联网法院审理“信息网络传播纠纷案”的做法,将涉案存证机构的股东及经营范围与原、被告是否有利害关系纳入审查范围。⑧此时,电子数据存证服务机构作为市场主体,不具有社会公共属性,是中立的第三方机构,应将区块链存证机构与普通第三方存证机构等同视之。

(二) 区块链存证电子数据的合法性审查

一般认为,证据的合法性应包括取证主体、取证程序、证据形式以及证据保全与运用的合法性。[18] 由此可知,与证据的真实性和关联性审查不同,证据的合法性认定不掺杂认定主体的个人价值评判,只要符合法律规定,而不问与案件事实的关联性。实际上,除了有违伦理道德的克隆等技术外,科技自身兼具客观性、中立性以及科学性特征,即科技本身存在自证功能,能够与法律之间建立天然的联系。只要法律确认区块链技术本身是合法的,那么区块链证据就当然具有合法性,只是现阶段的司法机关对区块链证据的出现尚无完善的应对之策,对其进行合法性认定也就成了必要程序之一,但不排除将来法律会认可科技的自证效力,从而免除区块链证据的合法性认定环节。就现阶段而言,一般证据的合法性审查标准也适用于区块链证据,不应为区块链证据专门设置合法性准入门槛,即只要符合《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》第 106 条的规定,即可认定区块链证据合法。

(三) 区块链存证电子数据的关联性审查

任何电子数据的产生都不是孤立的,电子数据的产生和存在具有多元化、系统化的特点。这种多元化和系统化具体体现为,用于证明待证事实的内容性电子数据,包括数据生成、存储、修改而形成的时间、修订次数等附属数据信息,以及记录了数据信息的发送人和接收人,日志记录、源代码等痕迹信息,这些信息都应一并保全,最大程度证明电子数据的真实性和与待证事实的关联性。[19] 具体操作标准就是,将网页自动抓取的能够清晰反映电子数据生成的原始介质、传递路径,以及其包含的痕迹信息与待证事实的关联性,同区块链上的时间戳信息具有同一性,即能够证明电子数据的真实性。在“信息网络传播案”中,当事人陈述、网页源代码以及自动抓取的侵权页面能够相互印证,反映了侵权链接的真实性,以较为完整的证据链印证了存证方式的可靠性,保证了电子数据的证明力。[20] 另外,还可以通过比较上传至区块链的电子数据哈希值与线下电子数据的哈希值是否一致,来鉴别电子数据是否真实完整。

结 语

基于区块链存证的电子数据在保留传统电子

数据特征的同时，实现了新科技对传统电子数据审查认定难题的重大突破：一方面，区块链技术的去中心化或分布式特征，化解了传统电子数据易被篡改的难题；另一方面，区块链本身具有不可篡改的特性，结合时间戳技术可以实现强大的自我背书，免去了公证环节，极大地降低了电子数据的技术鉴定成本，有效地改变了电子数据采信率低的现状。

自杭州互联网法院的区块链存证电子数据第一案以来，区块链存证电子证据在我国的互联网法院的司法实务中已经得到了较大发展。司法裁判的这种认可不但能够实现互联网环境下司法模式的创新，更可以进一步维护司法公正、提高司法效率。尽管只是个案，但证据法学理论的未来发展趋势已经能够预见，即证据的认定不但依赖于国家公权力的信用背书，而且在某些案件中，科学技术的客观性、中立性与科学性正逐渐被证据法理论所接受：一方面，适当破除传统证据认定规则的限制，遵从科学技术的客观中立性认定案件事实，有助于最大限度地减小证据认定过程中的主观误差；另一方面，法官只需判断电子数据的内容是否真实，而对于承载电子数据的科技载体，仅需查看专利证书并验证其具体功能便可证明其可信度。这对证据法理论的发展无疑是具有开创性的，同时也弥补了传统证据认定模式的不足。正如有论者指出，人工智能可以在法律适用问题上实现对法官的部分替代，而区块链技术可以在事实认定问题上实现对法官的完全替代，[21] 区块链技术在司法领域已经展现出巨大潜力，它能够把法官从事实认定难题中解放出来，是民事司法的一次生产力革命。

注释：

①参见杭州互联网法院（2018）浙0192民初81号民事判决书。

②参见青海省西宁市中级人民法院（2018）青01民终1474号民事判决书；江苏省淮安市淮阴区人民法院（2018）苏0804刑初132号刑事判决书。

③参见四川省成都市中级人民法院（2019）川01民终1050号民事判决书；重庆市第二中级人民法院（2013）渝中法民终字第01375号民事判决书；广东省广州市中级人民法院（2018）粤01民终23597号民事判决书。

④举例而言，《最高人民法院关于民事诉讼证据的若干规定》（2020年版）第23条。

⑤最高人民法院《关于民事诉讼证据的若干规定》（2020年版）第23条；《最高人民法院关于行政诉讼证据的若干规定》第12条。

⑥《最高人民法院关于〈民事诉讼法〉的司法解释》第104条。

⑦参见杭州互联网法院（2018）浙0192民初81号民事判决书。

⑧参见杭州互联网法院（2018）浙0192民初81号民事判决书。

参考文献：

[1] 张玉洁. 区块链技术的司法适用、体系难题与证据法革新[J]. 东方法学，2019(3).

[2] 刘品新. 印证与概率：电子数据的客观化采信[J]. 环球法律评论，2017(4).

[3] 刘哲玮. 民事电子数据：从法条独立到实质独立[J]. 证据科学，2015(6).

[4] 龙卫球，裴炜. 电子数据概念与审查认定规则的构建研究[J]. 北京航空航天大学学报（社会科学版），2016(2).

[5] 刘显鹏. 电子数据的证据能力与证明力关系探析——以两大诉讼法修改为背景[J]. 北京交通大学学报（社会科学版），2013(2).

[6] 袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016(4).

[7] 张偲. 区块链技术原理、应用及建议[J]. 软件，2016(11).

[8] 武源文，赵国栋，刘文献. 区块链与大数据：打造智能经济[M]. 人民邮电出版社，2017.

[9] 郑戈. 区块链与未来法治[J]. 东方法学，2018(3).

[10] 褚福民. 电子数据真实性的三个层面——以刑事诉讼为例的分析[J]. 法学研究，2018(4).

[11] 李静彧，李兆森. 基于区块链存证的电子数据真实性探讨[J]. 软件，2018(6).

[12] 侯义斌，梁勋，占小瑜. 基于区块链的电子数据系统架构模型[J]. 计算机科学，2018(6A).

[13] 刘品新. 论电子数据的理性真实观[J]. 法商研究，2018(4).

[14] 刘品新. 论电子数据的原件理论[J]. 法律科学，2009(5).

[15] 汪振林. 电子数据原件问题研究[J]. 重庆邮电大学学报（社会科学版），2012(5).

[16] 汪振林. 电子文书的原本性确保及其证明问题[J]. 重庆邮电大学学报（社会科学版），2011(5).

[17] 雷蕾. 从时间戳到区块链：网络著作权纠纷中电子存证的抗辩事由与司法审查[J]. 出版广角，2018(15).

[18] 刘方权. 双重视野下的证据合法性证明问题[J]. 中国刑事法杂志，2015(4).

[19] 李自柱. 第三方电子数据平台固定电子数据的调查研究[EB/OL]. 微信公众号：朝阳知产，2017-07-28.

[20] 卢忆纯. 区块链电子存证的法律效力认定[EB/OL]. http://www.sohu.com/a/248626935_221481，2019-03-02.

[21] 史明洲. 区块链时代的民事司法[J]. 东方法学，2019(3).

收稿日期 2020-10-26 **责任编辑** 苟正金