Doi:10.11835/j.issn.1008-5831.fx.2022.12.001

欢迎按以下格式引用:谢登科,张赫.电子数据区块链存证的理论反思[J].重庆大学学报(社会科学版),2025(2):241-252.
Doi:10.11835/j.issn.1008-5831.fx.2022.12.001.

Citation Format: XIE Dengke, ZHANG He. Theoretical reflection in the blockchain storage of electronic data as evidence[J]. Journal of Chongqing University (Social Science Edition),2025(2):241-252. Doi:10.11835/j.issn.1008-5831.fx.2022.12.001.

电子数据区块链存证的理论反思

谢登科,张 赫
(吉林大学 法学院,吉林 长春 130015)

摘要:鉴真是审查、认定电子数据真实性的重要手段,也是判断电子数据是否具备证据能力的前提要件。作为网络信息时代的"证据之王",电子数据在司法实践中应用范围越来越普遍,而电子数据所具有的易篡改性和虚拟性特征也给审查电子数据完整性、真实性工作带来挑战,如何保证电子数据在证据流转环节不被篡改、删减,既是电子数据鉴真的重点,也是电子数据鉴真的难点。借助分布式记账、非对称加密、可信时间戳等技术,区块链存证能够有效避免链上电子数据被任意篡改和删减,完成对上链存证的电子数据的鉴真工作。随着区块链存证技术在社会生活、工作领域中的应用越来越广泛,其与电子数据相结合,在实践中衍生出区块链电子数据这一新的电子数据表现形式。对此,有学者将区块链存证后的电子数据界定为区块链电子数据,探讨对该类电子数据进行鉴真的问题。但是,区块链电子数据并不等同于电子数据区块链存证,前者是电子数据的一种表现形式,后者是对电子数据进行鉴真的方法。区块链电子数据与电子数据区块链存证在存证时间、证据真实性、同一性和完整性的保障程度,与事实之间的关联性以及价值功能等方面都存在差异。因此,从区块链存证技术在二者中发挥的功能角度来看,若电子数据已通过区块链存证予以有效鉴真,就没有必要再次鉴真或重复鉴真;若对区块链存证后电子数据再次鉴真或重复鉴真,则其价值功能和正当基础就会削弱。作为鉴真方法的区块链存证与区块链电子数据对电子数据真实性、同一性的保障程度并不相同。将电子数据区块链存证等同于区块链电子数据,并对其进行鉴真这种理论误区产生的根源在于对区块链存证的认知存在偏差。区块链电子数据的产生依赖区块链技术的产生和发展,具有区块链技术的独特特征,而电子数据区块链存证中的电子数据生成过程与区块链无关,区块链存证平台只是保存、固定这类电子数据的工具,其并不会产生证明案件事实的新证据,它承担着与传统鉴真方法相同的诉讼功能,使电子数据鉴真从"系统推定真实"向"技术自证真实"方向扩展,推动电子数据鉴真方法朝着多元化方向发展。此外,作为电子数据技术性鉴真方法,区块链存证仅能为入链后电子数据的形式真实性提供保障,其并不否定对方当事人提出证据对该电子数据的真实性予以反驳和质疑。

基金项目:国家社会科学基金一般项目"电子数据区块链存证研究"(21BFX014);吉林省教育厅2023年度社会科学研究重大项目"吉林省在线诉讼规则适用实证研究"(JJKH20231101SK)

作者简介:谢登科,吉林大学理论法学研究中心教授,Email:xdkjlu@163.com。

关键词:电子数据;区块链存证;区块链电子数据;技术性鉴真;证据能力
中图分类号:D915.13 **文献标志码**:A **文章编号**:1008-5831(2025)02-0241-12

引言

作为网络信息时代的“证据之王”[1],电子数据在当代证据体系中占据重要地位。但是,电子数据具有虚拟性、易篡改性等特征,其在收集、提取、保存、流转等环节中,可能被破坏、篡改、删减进而产生失真风险。因此,鉴真就成为电子数据应用于诉讼证明和事实认定的必经环节。鉴真既是审查判断电子数据是否真实、有无被删减、篡改的重要手段,也是电子数据获得证据能力的基本前提。对此,为了提高对电子数据鉴真的效率和结果的可接受性,在司法实践中引入区块链存证技术成为一项革新电子数据鉴真方法的有效方式[2]。与传统鉴真方法不同,区块链存证技术以分布式记账、非对称加密、时间戳等信息技术为支撑,可以防止入链后电子数据被篡改,保障电子数据的真实性和同一性,实现对存证电子数据鉴真。但是,我国司法实务和理论中存在将“电子数据区块链存证”与“区块链电子数据”混同使用的情况,将“电子数据区块链存证”视为电子数据新的表现形式或者是新的证据类型,即区块链电子数据或区块链证据①;也有学者提出对区块链存证后的电子数据进行鉴真,即区块链电子数据的双重鉴真或双阶鉴真②。这些观点忽视了“电子数据区块链存证”与“区块链电子数据”之间的区别,混淆了区块链存证中的鉴真对象和鉴真方法,对电子数据区块链存证产生了多重认识误区。因此,有必要厘清“电子数据区块链存证”与“区块链电子数据”的概念,对现有电子数据区块链存证理论予以梳理和反思,科学界定和把握电子数据区块链存证的法律性质。

一、概念厘清:“电子数据区块链存证”与“区块链电子数据”

区块链技术在当下社会的使用范围越来越广泛,特别是在加密数字货币领域的应用,这的确会产生大量区块链电子数据,但并不能因此就将电子数据区块链存证纳入“区块链电子数据”之中。区块链电子数据是在区块链技术的基础架构和运行中所产生的电子数据的具体表现类型,区块链技术为此类电子数据的产生提供底层技术支撑。但是,区块链电子数据只是电子数据的表现类型发生了变化,其并没有创造出一种新的证据种类,本质上,区块链电子数据仍然是由0和1所组成的二进制编码,仍然属于电子数据范畴。电子数据区块链存证是将收集到的电子数据的哈希值存储在区块链网络之上,区块链技术对电子数据的形式真实性、同一性提供信任担保。“区块链电子数据”与“电子数据区块链存证”是两个概念,二者在价值功能、事实关联、生成节点等方面存在重大差异。下面将结合两个具体案例来界定和厘清二者关系。

案例一:李某与万科公司侵害作品信息网络传播权纠纷案③

李某发现万科公司在微信公众号上刊发了由其拍摄的照片且未注明照片出处和署名,遂通过

---

①参见:刘品新《论区块链证据》,载《法学研究》2021年第6期;丁春燕《区块链电子数据的证据能力分析——以农业保险欺诈刑事诉讼切入》,载《法学杂志》2021年第5期;刘学在,阮崇翔《区块链电子证据的研究与思考》,载《西北民族大学学报(哲学社会科学版)》2020年第1期;李忠操《国际商事诉讼中区块链技术证据的运用及中国因应》,载《法学杂志》2020年第2期。

②参见:段莉琼,吴博雅《区块链证据的真实性认定困境与出路》,载《法律适用》2020年第19期;龚善要《论区块链电子证据的双阶鉴真》,载《西安交通大学学报(社会科学版)》2021年第1期。

③详见:广东省广州互联网法院(2019)粤0192民初30162号民事判决书。

保全网对相关网页取证后予以区块链存证,存证类型为网页取证。法院对李某提供的证据予以审查,认为:原告通过保全网进行区块链网页取证,对侵权作品进行固定,其所采取的取证平台具备电子数据取证、存储的技术条件和符合国家技术资质要求,能够有效保证电子数据的真实、完整,故采信李某的诉讼主张。

案例二:胡均某与王桂某买卖合同纠纷案④

胡均某从王桂某处购买虚拟数字货币 TBToken 和比特币,后因付款发生纠纷而诉至法院。胡均某向法院提交了比特币交易平台账户记录,法院经审查后对其真实性予以确认。

在上述两案中,区块链技术的介入时间、价值功能并不相同,由此导致涉案电子数据的生成机制、利用区块链存证的时间以及在电子数据保存流转过程中区块链存证对保障电子数据真实、完整所发挥的功能也存在重大差别。案例一主要是将区块链技术作为电子数据存证的方法,通过利用区块链的技术特征保证链上电子数据不被他人任意篡改、删减。案例二是当下加密数字货币纠纷中较为常见的案例。在案例二中,区块链技术为加密数字提供底层技术支撑,加密数字货币从生成到交易、流通的整个环节都会被区块链上的各个节点记录下来并实时保存,这些基于区块链技术所产生的电子数据就属于“区块链电子数据”,案例二中的数字货币转账记录就是区块链电子数据的典型表现方式之一。“区块链电子数据”与“电子数据区块链存证”的差异主要表现在以下四个方面。

第一,区块链技术在二者中的价值功能发挥存在差别。在案例二中,加密数字货币及转账记录就是在区块链上产生,此种记录不仅能够用来证明加密数字货币交易事实的存在,其本身也是一种新型电子数据。此种电子数据依赖于区块链技术的产生与发展,若没有区块链技术,就不会产生“区块链电子数据”这一新型电子数据。在该类电子数据中,区块链技术具有证据生成和证据固定的双重功效:在证据生成方面,区块链技术是该类电子数据得以产生的基础和前提;在证据固定方面,该类电子数据自生成之后,同步入链存储,借助区块链防篡改的特征,保障链上生成电子数据的真实性。相比之下,在电子数据区块链存证中,电子数据的生成通常不涉及区块链技术,区块链本质上是一个对等网络的分布式账本数据库[3],区块链存证平台只是在电子数据保存流转过程中进行固定、保存的工具。作为存证对象的电子数据与存证方法的区块链技术相互分离,区块链技术仅在后期电子数据存证中得以运用。区块链技术不是伴随着案件发生而产生的证据材料,也不需要后续重新收集,其本身与案件事实不具有关联性。在案例一中,涉嫌侵权的微信公众号上发表的文章的制作和生成过程通常无需借助区块链技术,仅是后期存证中用到区块链技术。

第二,电子数据生成时间和存证时间存在差异。在电子数据区块链存证中,区块链存证和电子数据的生成通常不具有同步性,其通常发生在电子数据取证之后[4]。以案例一为例,李某提供证据证明万科公司网站存在侵权事实,这些证据是万科公司实施侵权行为时在网络空间所留下的“痕迹”,这类证据生成的系统环境与区块链技术无关。在案例一中,证明存在侵权事实的电子数据产生在先,区块链存证技术是李某将涉案电子数据的哈希值上链存储后才发生作用。而区块链电子数据生成于区块链技术环境系统之中,是当事人利用区块链网络所进行的日常数据处理行为,这些数据在生成的同时同步记录到区块链之中,电子数据生成和区块链存证具有同步性。作为建立在

④详见:北京市通州区人民法院(2019)京 0112 民初 37191 号民事判决书。

点对点网络结构上的区块链技术,可以利用分布式节点和共识算法来生成和更新数据,利用链式数据结构来验证和存储数据[5]。所以说,相较于电子数据区块链存证的阶段性特征,区块链电子数据通过算法程序自动上传至区块链中各个节点保存,此类电子数据存证具有同步性、全程性特征。区块链技术能够实现对电子数据生成、取证、举证等不同环节进行全流程存证,更好保障电子数据的完整性和真实性。

第三,区块链技术对电子数据真实性的保障程度不同。区块链电子数据的真实性具有更强保障,理由在于,区块链存证技术为该类电子数据的生成和存续提供底层技术支持,该类电子数据自生成的那一刻同步上链存储,链上电子数据是当事人对该电子数据处理行为的直观反映。这不仅提高了电子数据与案件事实之间的关联关系,也更好地保障了电子数据在保存和流转过程中的真实性和完整性。在案例二中,当事人通过出示加密数字货币转账记录、对方当事人数字货币钱包账户地址等证据向法院证明涉案争议数字货币交易行为存在,法院审查后,没有再借助其他证据来证明数字货币交易记录是否真实,而是直接根据当事人提供的证据材料认定案件争议事实。而在电子数据区块链存证中,区块链技术介入后,电子数据的生成流转过程被物理分割成“入链前”和“入链后”两个阶段[6],作为存证对象的电子数据属于链下生成的电子数据,由当事人或相关主体收集之后上传至区块链存证平台。这类电子数据由于生成环境与区块链技术无关,区块链存证仅能为入链后的电子数据的真实性、同一性提供担保,法官仍然需要审查该类电子数据在入链存储之前的保存、流转阶段是否存在被不当篡改、删减以及替换的风险。例如,在北京阅图科技有限公司与上海东方网股份有限公司著作权权属、侵权纠纷案中⑤,原告北京阅图科技有限公司利用区块链存证平台取证证明被告未经原告许可,在被告经营的网站上向公众传播原告享有著作权的作品。法院审理后指出,本案中原告所采取的可信时间戳取证无法排除取证网站虚假性、电子数据来源不真实的可能,故驳回原告诉讼请求。在该案中,法院在承认区块链存证平台对链上电子数据真实性保证的基础上,并没有直接采信当事人所提供的电子数据,而是通过审查涉案电子数据的来源以及当事人取证过程后指出,本案中当事人在用可信时间戳等技术手段采集证据时缺失关键步骤,导致无法确定接入网站的真实性,涉案电子数据来源真实性存在重大缺陷。与区块链电子数据不同,借助区块链存证平台所存储的电子数据都是在链下生成的电子数据,这类电子数据真实性和完整性决定了链上电子数据是否真实、完整。因此,对该类电子数据的审查判断需要结合其他证据进行综合判断。

第四,区块链技术对不同层级的事实发挥着真实性保障功效。根据证据材料证明的内容信息与涉案事实的远近关系,可以将证据材料所反映的事实分为一级事实和二级事实[7]。一级事实强调证据材料与案件事实之间的直接联系,其可以通过分析证据材料获得相关案件事实信息。二级事实独立于案件待证事实之外,是影响证据本身可信性的事实,它的作用在于通过引入外部证据对所主张证据的真实性进行证明。作为一种新型电子数据,区块链电子数据的证明对象直接指向案件事实,即案件的一级事实。以加密数字货币为例,用户在买入/卖出数字货币的时候,其一系列交易行为信息会被加上时间戳组合在一起形成一个信息块[8],并同时广播至链上节点,同步、真实、全面地反映交易流程。在争议发生时,区块链技术可将各类公共信息即原本孤立的证据点,梳理、连

⑤详见:北京市互联网法院(2019)京0491民初1212号民事判决书。

接成一条能够反映待证事实真伪的证据链[9],从而为查明事实提供依据和基础。在电子数据区块链存证中,作为存证对象的电子数据是被用来证明一级事实的证据,区块链存证作为技术工具本身并不能被用来证明案件的一级事实,它主要是用来保障案件二级事实的真实性,即利用区块链存证的技术特点确保入链后电子数据的真实性与同一性。例如,在案例一中,用来证明万科公司是否存在侵权事实的证据是侵权页面和网页源码,而保全网存储的由侵权电子数据计算生成的哈希值仅能为入链存储的电子数据的真实性和完整性提供保障,它属于确保案件二级事实的手段,即用来证明或保障电子数据真实性的方法,而不是用来直接证明案件事实的证据材料。

二、理论争鸣:电子数据区块链存证理论的双重误区

由于电子数据区块链存证的现有理论将其作为新型证据或电子数据——区块链证据[10],这必然会衍生出对区块链证据的鉴真问题,即对区块链存证后电子数据如何鉴真。但是,区块链存证本身就是电子数据的技术性鉴真方法,对所谓的“区块链电子数据”予以鉴真就会演变为对已经通过技术方法鉴真的电子数据予以鉴真的问题。从逻辑上分析,若对电子数据已经通过区块链存证方式予以有效鉴真,其自然没有再次鉴真或者重复鉴真的必要,否则,司法实践中大规模推行电子数据区块链存证的正当性和必要性就会大打折扣。此种悖论可能主要源于我国对电子数据区块链存证的理论误区。

(一)区块链存证的技术可靠性与鉴真标准的相对性

现有理论研究主要从区块链技术特点角度论证对区块链存证后电子数据进行鉴真的必要性和正当性。例如,区块链共识机制难以确保链上电子数据不被篡改[11]。也有学者从区块链“闭环安全”角度提出区块链节点之间的交易过程以及拥有的权益可能被黑客破坏,最终导致证据与事实的关系存在可能扭曲的危险[12]。上述观点将区块链的技术性缺陷作为对区块链存证后电子数据鉴真的正当理由。作为电子数据的技术性鉴真方法,区块链的这些技术性缺陷确实无法完全避免。但是,将这些技术性缺陷作为对区块链存证后电子数据予以鉴真的正当基础,有待进一步商榷。

首先,对电子数据进行鉴真的出发点是电子数据自身特点及其在收集、流转等环节存在的失真风险,而不是鉴真方法存在风险或缺陷。鉴真方法仅能为审查电子数据形式真实性提供基础材料和依据,其本身存在的技术性缺陷仅会阻碍对电子数据形式真实性的有效审查认定,但并不能作为对电子数据进行鉴真的正当事由,因为二者之间并不具有逻辑上的因果关系,当鉴真方法存在缺陷时,理应采取的措施是通过其他鉴真方法对此种缺陷进行及时弥补,确保电子数据鉴真结果的有效性。而且,鉴真方法的开放性特征也为引入多种方法对电子数据进行鉴真提供了可能。将区块链自身技术性缺陷和风险作为对存证电子数据鉴真的正当基础,实际上是将鉴真方法的可靠性作为对电子数据鉴真的理论前提,这与对电子数据鉴真的出发点相悖。在对实物证据进行鉴真的过程中,作为常见的鉴真方法,“保管链证明”和“独特性确认”在具体应用过程中同样也可能存在瑕疵或风险。以“保管链证明”为例,它要求接触实物证据的相关人员原则上都应出庭就证据保管的规范性、证据的真实性和关联性接受交叉询问[13]。其中存在接触实物证据的相关人员可能会因时间间隔过长而不能准确描述实物证据状况的风险。但是,此种风险并不能成为对实物证据鉴真的正当事由,实物证据鉴真的主要理由在于实物证据自身在收集、移送、保管等环节存在被调包或毁坏的风险[14]。作为电子数据技术性鉴真方法之一,区块链技术虽然也存在“51%攻击”等技术缺陷[15],

但是此种技术缺陷并不能成为对链上电子数据予以鉴真的正当事由。

其次,区块链技术风险低概率性与鉴真标准相对性的悖论。鉴真是对实物证据或电子数据真实性和同一性的证明,它是对实物证据或电子数据真实性和同一性的初步证明和筛查[16]。在美国证据法理论和司法实务中,对实物证据或电子数据鉴真的门槛或标准并不高,只需要达到《联邦证据规则》第901(a)条规定的"足以支持证明某项事实为真"(evidence sufficient to support a finding)标准[17],通过特定方法能够让法官相信某证据材料为真的可能性大于假的可能性,即可视为达到鉴真标准的要求。当前,虽然区块链技术尚未达到理论构想层面的绝对安全[18],在区块链存证具体应用过程中,确实存在链上数据被篡改的可能性。但是,区块链技术自身所嵌入的分布式账本、非对称加密等技术具有很高的安全性,任何一方想更改区块任意信息都必须重新对该区块以及其后所有区块进行哈希运算。以加密数字货币为例,攻击加密数字货币上的区块信息所需要的算力超过全球Top500超级计算机的算力总和[19],这就使得区块链技术风险事件发生的概率很低且成本极高,能保障链上数据不被任意篡改。因此,区块链存证通常可以达到电子数据鉴真的标准要求。在电子数据鉴真中,之所以要引入区块链存证技术,一方面源于该技术方法较为契合电子数据虚拟性、技术性等特征,另一方面是因为它可大幅降低对电子数据鉴真的难度与应用成本。一般来说,对于案件事实、证据真实性的证明标准设置越高,其所需要投入的诉讼资源也就越多。如果对通过区块链存证平台的电子数据进行再次鉴真,相当于变相提高了鉴真的标准和门槛,这不仅会导致与其他鉴真方法所要达到标准的不统一,也有悖于区块链存证旨在降低电子数据鉴真难度与成本的初衷。

最后,区块链技术风险发生的低概率性与鉴真规则适用常态性之间存在悖论。鉴真是审查认定实物证据是否具备可采性的前提[20],在电子数据审查认定过程中具有常态性,当事人向法院提出某一电子数据来支持己方诉讼主张时,他首先应当提供某种方法或材料来证明该电子数据是其所主张的电子数据。结合前文,区块链技术自身所嵌入的分布式账本、可信时间戳、非对称加密等技术具有很高的安全性,通常可以满足电子数据鉴真的需要。在区块链技术已经保证电子数据真实性的前提下,基于其所具有的技术风险对链上电子数据进行二次鉴真就应当具有例外性,以有证据证明该风险会使法官对电子数据真实性产生怀疑为前提。如果将发生概率较低的区块链技术风险作为对存证电子数据鉴真的理论依据,意味着不论是在区块链电子数据还是在电子数据区块链存证中,对链上电子数据的二次鉴真应当属于常态而不是例外,这显然就与电子数据鉴真规则的常态适用相悖。

当然,区块链技术风险发生的概率虽然较低,但在实践运行中仍然有可能发生。作为电子数据的技术性鉴真方法,区块链的技术风险若实际发生,就可能无法对链上电子数据进行有效鉴真。在现有鉴真规则制度和理论系统中,对已有鉴真方法存在的瑕疵或问题,允许通过事后鉴真方法来弥补。比如在快播公司传播淫秽物品案中,执法机关在扣押涉案服务器时未作封存处理,辩护方提出服务器中存储的电子数据来源不明,硬盘可能被污染、调换,不应作为证据认定;法院则委托鉴定机构对服务器中电子数据是否存在从外部拷入或修改的问题进行鉴定,最终采信了该电子数据⑥。这就是通过事后鉴定鉴真来弥补"证据保管链"瑕疵,实现对电子数据有效鉴真的典型案例。事后鉴

⑥详见:北京市海淀区人民法院(2015)海刑初字第512号刑事判决书;北京市第一中级人民法院(2016)京01刑终592号刑事裁定书。

真方法主要是对事前鉴真方法已经发生瑕疵或问题的补救,并不着眼于对尚未发生风险的预防。“快播”案中法院之所以对电子数据进行鉴定,是因为执法机关没有对扣押的服务器予以封存处理,“证据保管链”存在瑕疵,这种瑕疵导致无法通过“保管链证明”方法对电子数据予以有效鉴真。在司法实务中,事前鉴真方法中的瑕疵并不总会出现。因此,事后鉴真方法的适用就具有救济性、或然性,区块链技术风险的低概率性使未实际发生的风险并不会导致已存证电子数据无法有效鉴真,基于对技术信任的考量,不需要再对链上电子数据进行事后鉴真。

(二)电子数据区块链存证中的鉴真对象与鉴真方法

现有电子数据区块链存证理论,主张将区块链存证平台界定为电子数据外在载体进而将其作为鉴真对象[12]。此观点有待商榷,其不仅从电子数据与其存储介质相互关系层面混淆了鉴真对象,也混淆了鉴真对象和鉴真方法审查之间的关系,并且容易导致对电子数据区块链存证陷入法律性质认识误区。

首先,区块链存证是一种“去外在载体化”或“去存储介质化”的电子数据鉴真方法,通过区块链存证进行鉴真的对象指向电子数据本身,不需要对其存储介质或者是存储载体进行鉴真。结合电子数据所具有的虚拟性特征,需要借助于特定存储介质来存储、流转,因此电子数据传统鉴真方法主要采取“存储介质+电子数据”的双重鉴真[21],既要对电子数据存储介质鉴真,也要对其中存储的电子数据鉴真。不论是通过“一体收集”模式将电子数据与其存储载体一并收集,还是借助“单独提取”模式将电子数据从原始存储载体中提取出来后拷贝到其他存储介质之中,都需要对电子数据所依附的存储介质进行封存、记录[22]。但是,电子数据也具有可复制性、相对可分离性,其数据信息并非必然要依附于其原始存储介质而存在,这就意味着对其存储介质的鉴真并不能必然保证其内部存储的电子数据的真实性。摆脱对电子数据存储介质鉴真的依附,实现对其自身独立的鉴真,就成为当下电子数据鉴真的发展趋势。区块链存证就是一种“去载体化”的电子数据鉴真方法,不管是区块链存证还是区块链电子数据,实际上并不存在所谓的数据载体,链上数据与其承载的内容信息之间的界限难以区分[23]。区块链存证通过非对称加密方式等实现对电子数据自身表征,然后将此种表征信息同步上传至区块链中予以分布式存储,进而为法庭审理过程中电子数据鉴真奠定基础。在这个过程中,区块链存证实现了对电子数据独立化、去存储介质化鉴真。法院借助区块链存证平台在线对比哈希值就可以直接实现对存储电子数据自身真实性进行审查,无需再审查其原始存储器介质。比如在案例一中,法院审查后直接采纳保全网存储电子数据的真实性,而没有继续对保全网的服务器进行鉴真。

其次,区块链存证可以实现对电子数据独特性的表征,此种表征功能无需借助于电子数据的存储介质即可实现。作为传统实物证据鉴真主要方法的“保管链证明”和“独特性确认”,通常需要以证据的某些特征或独特性为基础,这些特征可以是证据自带的,比如指纹;也可以是人为设置的,比如作特定标识[24]。以“证据保管链”为例,需要在收集、流转、保管等环节对证据名称、特征等信息予以详细记载,为事后比对、认定实物证据的真实性奠定基础。由此可见,传统实物证据的特征会体现在其物质形态或载体之中,实物证据的某些特征或独特性可以为其鉴真奠定基础。因此,对电子数据也可以创设其独特性特征,作为判断其真实性的参照。比如电子数据的哈希值,它是对任意长度的输入数据通过散列函数算法变换为固定长度的输出值,具有唯一性和确定性,两个不同数据经过哈希函数运算得到的哈希值不同,对同一数据输入或相同数据输入,无论经多少次哈希函数运

算,得到的哈希值都相同[25],因此也被称为“数字DNA”“数字指纹”[26]。在区块链网络中,电子数据无法直接存储到区块链网络上,而是在计算电子数据的哈希值后,将相对应的哈希值上链存储。此时,哈希值具有不可逆性,无法通过哈希值直接感知电子数据所呈现的证据信息内容,但其唯一性和确定性可以为电子数据自我鉴真奠定基础,因为对电子数据的任何细微改动或增减都会导致哈希值发生变化。因此,通过区块链中分布式存储的哈希值可以实现对电子数据独特性的表征。而电子数据的此种独特性特征,是独立于其存储介质,与其所处于何种存储介质没有任何关系。

最后,对电子数据区块链存证平台的审查并不属于电子数据鉴真范畴,其本质上是对鉴真方法可靠性的审查。在对传统实物证据进行鉴真的过程中,常见的鉴真方法如“保管链证明”和“独特性确认”是借助取证笔录、相关证人证言等方法对实物证据进行鉴真。对于取证笔录或相关证人证言,法院并非不作任何审查就直接将其作为认定实物证据形式真实性的依据,在借助这些方法对实物证据进行鉴真时,法院也需要对其可靠性予以审查,但是这并不意味着作为法院审查对象的取证笔录或相关证人证言就属于鉴真对象,它们仅仅是法院用来对实物证据鉴真的方法。法院对电子数据区块链存证的审查认定中亦是如此。对于电子数据区块链存证,法院也需要对存证主体是否具有法定资质、存证过程是否符合相关技术标准等因素予以审查⑦,但这并不是要将存证平台作为鉴真对象,而仅仅是将其作为对电子数据鉴真方法的审查。作为鉴真对象的电子数据,法院通常有义务主动审查其真实性,提供电子数据的当事人也有义务主动提供相应材料或方法来证明其真实性。而作为鉴真方法的区块链存证平台,仅在对方当事人对存证平台的可靠性提出合理质疑时,法院才有义务主动审查其可靠性。

三、性质探析:作为技术性鉴真方法的区块链存证

作为广义的实物证据,电子数据在诉讼程序中的审查和认定也需要遵循实物鉴真规则,对电子数据的鉴真过程不论是在价值功能判定方面还是在鉴真标准审查方面与传统实物证据鉴真之间并不存在差别。但是,由于电子数据在证据形态、取证方式等方面与物证、书证等传统实物证据差别较大,因此,对电子数据所采用的鉴真方法与传统实物证据并不完全相同。对电子数据进行鉴真,除了可以采取传统的“保管链证明”和“独特性确认”方法外,也可以借助网络信息技术手段实现对电子数据真实性审查,这其中就包括区块链存证。从法律性质来看,区块链存证本质上是电子数据的技术性鉴真方法[27],这主要基于以下理由。

第一,区块链存证可以为认定电子数据真实性和同一性提供基础材料或方法,其承担着与“保管链证明”和“独特性确认”等传统鉴真方法相同的诉讼功能。

实物鉴真规则的基本要求需要由实物证据的提出者来证明该实物证据就是其所主张的证据,在保存、流转过程中没有被改变或替换。例如,证据提出者可以通过提出某项证据完整的保管记录文件或者是某项证据所具有的独特特征来证明庭审中出示的物证与原来的物证具有同一性。区块

⑦《人民法院在线诉讼规则》第17条:当事人对区块链技术存储的电子数据上链后的真实性提出异议,并有合理理由的,人民法院应当结合下列因素作出判断:(1)存证平台是否符合国家有关部门关于提供区块链存证服务的相关规定;(2)当事人与存证平台是否存在利害关系,并利用技术手段不当干预取证、存证过程;(3)存证平台的信息系统是否符合清洁性、安全性、可靠性、可用性的国家标准或者行业标准;(4)存证技术和过程是否符合相关国家标准或者行业标准中关于系统环境、技术安全、加密方式、数据传输、信息验证等方面的要求。

链存证在电子数据鉴真中的应用,主要源于其具有对入链存证数据的防篡改功能,所有上传至链上的数据都会自动生成时间戳,这种单项加密手段使得无法通过技术手段修改已经加密的结果[28],防止入链存证的电子数据被任意篡改或删除。因此,区块链存证承担着与“保管链证明”和“独特性确认”等鉴真方法相同的诉讼功能,它们都是为电子数据的真实性和同一性证明提供材料或方法,消除各方当事人对电子数据真实性和同一性的争议,为法院认定该电子数据真实性奠定基础。但是,传统的“保管链证明”和“独特性确认”两种鉴真方法主要是通过有关人员的记录或陈述来为证明实物证据的真实性和同一性提供材料,它们具有“人际信任”的内在鉴真逻辑,在鉴真过程中难以摆脱相关人员认识能力、记忆能力、表达能力等主观因素的影响。而区块链存证是借由算法程序将电子数据转化成固定的哈希值,只要电子数据不发生变化,其哈希值就不会发生变化,它具有“机器信任”的特点,可以降低鉴真过程中第三方主体主观因素影响,对电子数据真实性和同一性的保障效果更佳。

第二,鉴真方法的开放性与灵活性为引入区块链存证奠定了制度空间,实现电子数据鉴真从“系统推定真实”向“技术自证真实”的扩展。

由于实物证据形态的多样性和案件事实的差异性,司法实践中对实物证据鉴真所采用的鉴真方法并不固定,而是具有灵活、开放的特点[29]。美国《联邦证据规则》第 901(b)条列举了包括“知情证人的证言”“关于笔迹的非专家意见”“专家证人或者事实审判者所进行的比对”等在内的多种鉴真方法,在法庭审理过程中,具体适用何种鉴真方法,需要结合案件具体情况灵活选择[30]313。这种对鉴真方法开放式的列举规范为引入新的鉴真方法奠定了制度空间,为电子数据鉴真方法朝着多元、开放、技术性方向发展扫清了制度上的障碍。传统鉴真方法在电子数据真实性审查认定中发挥作用的同时,由于完整性校验值、可信时间戳等技术鉴真方法所具有的便利性和有效性,逐渐被司法工作人员、当事人、律师们所接受,在电子数据鉴真中的使用也越来越广泛。例如,美国《联邦证据规则》第 901(b)条第 9 项规定“表明系统或程序能产生准确结果的证据材料”,可以作为电子数据的鉴真方法之一。此时,电子数据鉴真并非依据其自身特征,而主要是结合计算机系统或程序的稳定性、数据形成的可重复性来推定电子数据具有真实性,即数据输出结果的可检验性作为电子数据鉴真的基础依据[31]。2017 年 12 月,美国《联邦证据规则》第 902 条在原有自我鉴真条款的基础上增加了第 13、14 项,明确了电子数据自我鉴真的两种新方法。其中,第 14 项规定对于从电子设备或存储介质中复制的数据,若已由适格人员经相应数字认证程序或方法予以认证,就可以实现自我鉴真。该规则就允许当事人依据普遍接受的标准或方法来便捷、快速地证明电子数据真实性[32]。这些方法主要包括完整性校验值、数字签名、区块链存证等技术手段。2019 年 3 月,美国佛蒙特州将区块链记录作为电子数据自我鉴真方法在《佛蒙特州证据规则》中予以明确规定,证据提出者可以从数据入链时间、区块生成时间、区块链记录阶段等方面审查区块链存证电子数据的真实性。若符合法定条件,区块链存证电子数据则满足自我鉴真的要求,可以直接认定其具有形式真实性和同一性。我国最高人民法院 2021 年出台《人民法院在线诉讼规则》第 16 条明确了区块链存证后电子数据的法律效力⑧,对于区块链存证的电子数据,经技术核验一致的,原则上可以推定其具有真实性

⑧《人民法院在线诉讼规则》第 16 条:当事人作为证据提交的电子数据系通过区块链技术存储,并经技术核验一致的,人民法院可以认定该电子数据上链后未经篡改,但有相反证据足以推翻的除外。

和同一性,这实际上已经赋予区块链存证对电子数据的鉴真效力。但是,相对于通过电子数据运行的计算机系统或程序稳定性来推定其真实性的技术性鉴真方法,区块链存证则主要是通过电子数据完整性校验值的分布式存储和智能合约自动比对来审查电子数据的真实性和同一性,实现了电子数据技术性鉴真方法从“系统推定真实”向“技术自证真实”的扩展。当然,区块链存证作为电子数据自我鉴真的技术性方法,也仅能实现对电子数据形式真实性和同一性的认定,而对于其实质内容的真实性,仍然需要结合案件其他证据材料综合判断。

鉴真作为审查电子数据是否具备证据能力的要素之一,对已经通过有效鉴真且符合证据能力规则要求的电子数据,仍然允许对方当事人提出证据对真实性予以反驳和质疑。但是,此时该方当事人所提出的证据是用于攻击所采证据的证明力或可信性[31]325。例如,在 Frank R. Whitaker v. US 案中,辩护方基于计算机记录存在被篡改的可能性,主张控诉方提交的电子数据不符合证据鉴真规则要求。联邦上诉法院认为,对计算机文件存在被篡改的可能性不过是一种没有任何证据支持的假象,在缺乏明确证据证明发生了篡改的情况下,仅以存在篡改的可能性并不影响计算机记录具备自我鉴真的要求[33]。在 Novak v. Tucows 案中,法院指出在证据具备自我鉴真功能的情况下,以没有经过鉴真审查的互联网网页内容记录不具有真实性而主张证据不可采的,应由互联网存档系统的雇员明确指出该内容记录确系被篡改[34]。在电子数据区块链存证中,当事人将电子数据哈希值上传至存证链上之后,广播至链上节点,每个区块会被自动标记一个时间,表明该数据写入时间,即时间戳。相较于链上数据内容需要由用户主动上传,时间戳系数据被写入时自动生成,结合区块链分布式存储特点,电子数据区块链存证具备自我鉴真的效果。对于通过区块链存证而予以有效自我鉴真的电子数据,仅意味着其具备了形式真实性,对方当事人仍然可以从实质真实性层面对电子数据予以反驳和质疑。

第三,作为鉴真方法的区块链存证仅能保证入链后电子数据的形式真实性和同一性,而无法为其合法性与关联性提供背书。

作为定案依据的电子数据应当具有真实性、关联性和合法性,而区块链存证仅能为入链后电子数据的形式真实性和同一性提供保障,通常不涉及电子数据取证过程的合法性,也不能为电子数据关联性提供背书。证据合法性主要包括取证主体合法、取证程序合法和证据形式合法三个方面,其中主要是取证程序的合法性[35]。在电子数据区块链存证中,区块链存证发生于电子数据取证之后,区块链存证既不会减损依照法定程序收集电子数据的合法性,也无法修复违反法定程序收集电子数据的非法性。在电子数据收集提取和审查认定中,需要遵循相应证据规则。这些证据规则有些是为了保障证据的真实性和可靠性,比如原件规则和鉴真规则;有些是为了保障证据所承载的基本权利,比如非法证据排除规则[36]。区块链存证作为实现电子数据鉴真的技术方法,仅承担保障入链电子数据不被篡改或替换的功能,指向入链后电子数据的真实性或可靠性,区块链存证并不能为入链前取证行为的合法性提供背书。比如,通过木马程序非法侵入他人邮箱所收集的电子邮件、通过非法手段所获取的个人信息等非法电子数据,在上传至司法区块链平台存证之后,非法证据并不会因为区块链存证而被“漂白”为合法证据,非法电子数据也并不会因披着区块链存证的“外衣”而成为合法证据。区块链存证本身并不能改变违法取证的既定事实,也无法为非法取证行为所侵害的公民基本权利提供有效救济。对于电子数据的关联性亦是如此,区块链存证也不能解决电子数据的关联性问题。比如当事人超范围收集的、与案件无关的电子数据,并不会因为对其予以区块链存

证就会让其获得关联性;当事人所收集与案件有关的电子数据,也不会因为区块链存证而减损其关联性。因此,区块链存证的电子数据并不具有“天然合法性”或“天然关联性”,法官在区块链存证电子数据审查认定中仍然需要审查其合法性与关联性。

参考文献:

[1] 刘品新. 电子证据的基础理论[J]. 国家检察官学院学报,2017(1):151-159.

[2] 陈爱飞. 电子数据区块链存证的法律规制:基于66份判决书的分析[J]. 苏州大学学报(哲学社会科学版)2022(5):85-97.

[3] 邹均, 张海宁,唐屹,等. 区块链技术指南[M]. 北京: 机械工业出版社, 2016:92.

[4] 谢登科. 电子数据区块链存证的法律本质与适用边界[J]. 兰州学刊,2021(12):5-15.

[5] 赵刚,张健. 数字化信任:区块链的本质与应用[M]. 北京:电子工业出版社,2020:59-60.

[6] 李海鑫. 电子数据区块链鉴真的中国路径[J]. 学术交流,2024(2):80-92.

[7] 牟绿叶. 论实物证据的鉴真与鉴定:以美国法为参照的分析[J]. 中国司法鉴定,2012(3):25-30.

[8] 潘文博. 数字货币的运行机制与法律治理[J]. 清华法学,2023(2):75-89.

[9] 李忠操. 国际商事诉讼中区块链技术证据的运用及中国因应[J]. 法学杂志,2020(2):122-132.

[10] 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):99-109.

[11] 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):145-152.

[12] 杨继文. 区块链证据规则体系[J]. 苏州大学学报(哲学社会科学版),2021(3):86-95.

[13] 陈永生. 证据保管链制度研究[J]. 法学研究,2014(5):175-191.

[14] 陈瑞华. 实物证据的鉴真问题[J]. 法学研究,2011(5):80-92.

[15] 沈鑫,裴庆祺,刘雪峰. 区块链技术综述[J]. 网络与信息安全学报,2016(11):11-20.

[16] 孙锐. 实物证据庭审质证规则研究:以美国鉴真规则的借鉴为视角,安徽大学学报(哲学社会科学版),2016(4):136-144.

[17] 陈邦达. 美国鉴真规则及其借鉴价值[J]. 证据科学,2020(5):560-572.

[18] 龚善要. 电子证据区块链存证的功能厘清与实践应用[J]. 大连理工大学学报(社会科学版),2023(5):111-119.

[19] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016(11):481-494.

[20] 李戈. 数字时代刑事电子数据鉴真的模式选择[J]. 济南大学学报(社会科学版),2023(3):150-160.

[21] 刘译矾. 论电子数据的双重鉴真[J]. 当代法学,2018(3):88-98.

[22] 谢登科. 电子数据的鉴真问题[J]. 国家检察官学院学报,2017(5):50-72,174.

[23] 刘品新. 论区块链证据[J]. 法学研究,2021(6):130-148.

[24] 刘品新. 电子证据的鉴真问题:基于快播案的反思[J]. 中外法学,2017(1):89-103.

[25] 谢登科. 电子数据的技术性鉴真[J]. 法学研究,2022(2):209-224.

[26] 麦永浩. 电子数据司法鉴定实务[M]. 第2版. 北京:法律出版社,2019:5.

[27] 谢登科. 电子数据的技术性鉴真[J]. 法学研究,2022(2):209-224.

[28] 苗泽一. 论区块链技术的应用与规制:从“腾讯诉老干妈案”谈起[J]. 重庆大学学报(社会科学版),2023(1):228-240.

[29] 吴洪琪. 电子数据完整性的法律定位与理论反思[J]. 国家检察官学院学报,2024(1):146-160.

[30] 王进喜. 美国《联邦证据规则》(2011年重塑版)条解[M]. 北京:中国法制出版社,2012:313,325.

[31] 罗纳德. J. 艾伦,理查德. B. 库恩斯,埃莉诺·斯威夫特. 证据法:文本、问题和案例[M]. 张保生,王进喜,赵滢,译. 北京:高等教育出版社,2006:229.

[32] SCHUPANITZ A,CHOU J L. Judges’ treatment of federal rules of evidence 902(13) and 902(14)[J]. Department of Justice Journal of Federal Law and Practice,2020(5):109-129.

[33] 何家弘. 美国电子证据规则[M]. 北京:中国检察出版社,2004:39.

[34] KAREN G. Authenticity of archived websites:The need to lower the evidentiary hurdle is imminent[J]. Rutgers Computer and Technology Law Journal,2013(39):216-245.

[35] 戴长林. 非法证据排除规定和规程理解与适用[M]. 北京:法律出版社,2019:12.

[36] 孙远. 刑事证据能力导论[M]. 北京:人民法院出版社,2007:40.

Theoretical reflection in the blockchain storage of electronic data as evidence

XIE Dengke, ZHANG He

(*School of Law, Jilin University, Changchun 130015, P. R. China*)

Abstract: Authentication is an important way to exam and identify electronic evidence, and it's also a prerequisite for judging the evidence capability of electronic evidence. As the king of evidence in the age of network information, electronic evidence is being used in an increasingly wide range of judicial practices. However, electronic evidence is virtual and is easily tampered with, which makes the examination of the completeness and authenticity of electronic evidence more difficult. How to ensure that electronic evidence will not be tampered with or deleted in evidence circulation is the important and difficult points in authentication. Because distributed ledger, asymmetric cryptographic algorithm, timestamp and other technologies are embedded in blockchain storage, the electronic evidence can't be tampered with and deleted after entering the blockchain, and the work of authentication can be accomplished. With the increasingly widespread application of blockchain storage technology in social life and work areas, its combination with electronic evidence derives the electronic evidence of blockchain, a new type of electronic evidence. Some scholars take the blockchain storage of electronic evidence as electronic evidence of blockchain, and discuss the authentication of such electronic evidence. But the two are different, with the latter a type of electronic evidence and the former a way of authentication. In addition, they are differing in the time of evidence preservation, degree of authenticity and identity, factual relevance, value function and so on. Thus, from the perspective of the function of blockchain storage, if the electronic evidence has been authenticated, it doesn't need to be authenticated again. If we authenticate it again, the legitimacy and necessity of implementing the blockchain storage of electronic evidence in judicial practice will be greatly reduced. As a way of authentication, blockchain storage is differ from electronic evidence of blockchain in terms of authenticity and identity. This misconception taking blockchain storage as electronic evidence of blockchain and authenticating it stems mainly from theoretical misunderstanding of the blockchain storage of electronic evidence. The generation of electronic evidence of blockchain depends on the generation and development of blockchain technology, and has the unique characteristics of blockchain technology. The generation of electronic evidence which is storaged by blockchain aren't depend on the blockchain technology. The blockchain storage platform is the tool for preserving and fixing the electronic evidence, which will not generate new evidence to prove the facts of a case. It undertakes the same functions as traditional authentication methods, which makes authentication about electronic evidence move from systematic presumption of authenticity to self-attestation of authenticity by technology, and promotes the diversified development of electronic evidence authentication. What's more, blockchain storage of electronic evidence can only provide guarantee for the formal authenticity of electronic evidence entering the blockchain and the opposite party also can challenge the authenticity.

Key words: electronic data; blockchain storage; electronic data of blockchain; technical authentication; evidence capability

(责任编辑 刘 琦)