区块链存证电子证据鉴真现状与规则完善

伊 然

【摘 要】2021年5月18日最高人民法院审判委员会审议通过的《人民法院在线诉讼规则》第16条再次明确区块链技术存储电子数据[①]的效力。早在2018年9月7日施行的《最高人民法院关于互联网法院审理案件若干问题的规定》第11条就首次确认,电子签名、可信时间戳、哈希值校验、区块链等可作为验证电子数据真实性的技术手段,2020年5月1日实施的《最高人民法院〈关于民事诉讼证据的若干规定〉》更是在第93、94条中专门规定了判断电子证据真实性的条文。然而,区块链技术存储的电子证据何以获得证据能力、真实性如何正确认定一直是困扰司法实践的核心问题。以互联网法院建设的区块链进行实证考察,透过电子证据特点,结合区块链技术特征,解构经该方法存储的证据何以自我鉴真及认证法理基础,对于数字时代平衡司法公平与效率,具有深刻意义。

【关 键 词】电子数据;真实性;区块链技术;司法领域;鉴真

【作者简介】伊然,北京互联网法院四级高级法官。

【原文出处】《法律适用》(京),2022.2.106~117

一、问题提出:区块链证据司法实践现状检视

疫情常态化和不稳定化给全球经济带来了不确定性,原本的社会秩序发生重大变化。与此同时,我国已经全面进入移动互联网时代,信息技术深刻改变了人们的生产和生活,这也给司法带来了前所未有的机遇和挑战。面对新要求和新挑战,人民法院加速推进智慧法院建设,传统的审判流程从线下转移到线上,数据信息从纸面转移到“云端”或“链上”,审判各诉讼环节都发生了深刻变化,以计算机及其网络为依托的电子证据在证明案件事实的过程中起着越来越重要的作用。而电子证据的区块链固定方法[②]也成为电子证据最为常用的存证手段。

(一)区块链生态逻辑的司法体现:“存”与“取”

区块链的信息储存与证明功能可以说是目前区块链相关衍生应用中获得行业认可程度最高的功能之一。杭州互联网法院、北京互联网法院、广州互联网法院相继上线运行司法区块链,解决电子存证的难题。

司法区块链并不是一个法律概念,仍属于行业发展中形成的称谓。一般是指由法院主导建立的存证、取证的区块链平台,大多属于联盟链,法院节点一般为管理共识节点,也有法院作为其中一个普通共识节点的情形。如北京互联网法院的天平链,北京互联网法院的节点为管理节点,而北京市高级人民法院的节点为其中一个参与接入的节点。

以天平链为例,自2018年9月9日上线,截止至2021年5月10日,前十名的存证接入主体和调取证据的接入主体如下页表所示。

作者曾于2019年调研[③],发现由法院参与或者主导的区块链平台无论是业界还是法院,普遍认为可

表1 2018年9月9日–2021年5月10日存证TOP 10

接入方	存证总数	调证数量	类型
国网电商	8366354	131	
北京共识数信科技有限公司	6427268	1	版权数据
真相科技	4213338	93	
百度	4100402	1272	
京东智臻链	3889550	393	版权数据
中海义信	2847843	817	版权数据
安妮股份	2574890	1749	版权数据
信任度	588596	5679	电子合同
京市高级人民法院电子诉讼平台	241870	6	
中国搜索	208541	155	版权数据

表2 2018年9月9日–2021年5月10日调证TOP 10

接入方	存证总数	调证数量	类型
信任度	588596	5679	电子合同
安妮股份	2574890	1749	版权数据
百度	4100402	1272	
中海义信	2847843	817	版权数据
京东智臻链	3889550	393	版权数据
方圆公证处	15493	245	版权数据
中国搜索	208541	155	版权数据
国网电商	8366354	131	
中信梧桐港	51382	126	
真相科技	4213338	93	

信度较高，尤其是当事人通过该法院主导的区块链平台存证的，该法院在认定该证据时，对于真实性几乎不存在质疑。这一调研结论恰巧与天平链存证数据所呈现出的结论一致——司法区块链证据存储率高而调取率低。

“存高、取低”的现状，从表象上，反映出随着数字经济和移动互联网的发展，越来越多的当事人意识到数据及时上链或者直接让电子证据产生之初即刻上链的必要性。实质上，反映出当事人在遵循证据法的逻辑来有意识地准备为自己“预存”证据以应对将来可能的诉讼风险。然而，这种“存高、取低”的背后可能还隐藏着“多版本预留”原始恶意，即当事人就某一事实随着发展变化形成的一系列电子证据的多个“版本”分别上传至区块链存证，当争议发生时，选择有利于己方“版本”的电子证据作为证据提交法庭。

区块链技术应用于司法存证，不但冲破时间对数据保留的掣肘，分布存储的特性还打破了空间对数据存储的限制，然而这种技术的发展并不会遵从证据法设定的证明逻辑来演进。

(二)区块链技术逻辑的司法困惑：“法”与“技”

截至2021年6月，以“区块链”为关键词对中国

裁判文书网中生效民事裁判文书进行全文检索，文书为1813份。其中，以关键字排名前二名的是“合同”690份和“侵权行为”416份，以案由排名前二名的二级案由[④]是：“合同纠纷”998份，“知识产权权属、侵权纠纷”432份；进一步细化发现“合同纠纷”项下文书最多的案由是“借款合同纠纷”，有296份，而“知识产权权属、侵权纠纷”项下文书最多的案由是“著作权权属、侵权纠纷”，有341份。通过粗略的梳理[⑤]就会发现使用区块链存证的案由基本集中在侵权纠纷中的“著作权权属、侵权纠纷”。

从裁判文书出具年份来看，剔除无效样本后[⑥]共涉及5个年份：2017年17份、2018年149份、2019年630份、2020年876份、2021年140份，将2021年非整年样本排除后发现，涉及区块链的文书样本逐年升高。

再以上述样本中高频存证平台名称作为关键词检索并随机选取2019年-2021年期间各地法院的论述，剔除掉被告方直接认可的样本后如下表所示。

IP360真相科技	(2019)粤0305民初23896号[采信]	2019年11月26日	1.平台资质审查 2.环境的情节性审查、电子数据形成时间的准确性。
IP360真相科技	(2018)京73民终2163号[采信]	2020年12月30日	1.关于存证平台的资质审查：……其运营的IP360数据权益保护平台通过了公安部安全与警用电子产品质量检测中心和国家安全防范报警系统产品质量监督检验中心(北京)的检验认证，具备作为第三方电子存证平台的资质。 2.关于电子数据生成及储存方法可靠性的审查：……保证了电子数据形成时间的准确性，避免了对本地系统预先清洁以保证取证环境真实性的问题。 3.关于保持电子数据完整性方法可靠性的审查：……此种方式通过密码技术及数字指纹异地同步，可以保证电子数据的完整性。
易保全	(2019)湘知民终441号[未采信]	2019年12月16日	1.仅能证明电子副本与留存于服务器上的电子数据一致，而不足以证明其留存于服务器上的电子数据形成过程中操作环境是否清洁，取证方式是否规范，取证结果是否真实、完整，取证结果上传服务器之前是否经过篡改。 2.在缺乏技术说明和印证证据的情况下，不足以自证该时间就是保全行为发生的真实时间。 3.与公证机构的公证行为相比，重庆易保全网络科技有限公司取证的证据并不具有法律预设的证明力。
易保全	(2019)闽民终471号[采信]	2019年6月10日	1.取证行为系依靠第三方重庆易保全网络科技有限公司的易保全《电子数据保全平台》对互联网数据进行的保全和固化，并获得了《电子数据取证证书》。 2.太昊公司没有提供相反证据的情况下，应当认定全景视觉公司提供的证据真实有效。
易保全	(2020)川知民终557号[采信]	2020年12月30日	未论证
易保全	(2020)湘01民终12762号[采信]	2020年12月30日	1.虽然重庆易保全网络科技有限公司并非公证机构，其出具的电子数据取证证书也非公证书，但可按照电子数据的性质对其进行审查，经审查该电子数据取证证书及附件视频可完整、客观的展现取证环境、取证时间、取证过程与取证结果，在上诉人经营的网站店铺上可以清晰地看到涉案图片以及上诉人企业信息。 2.无相反证据证实的前提下，本院认定春盛中药饮片公司在其运营的网站中使用了被控侵权图片。
易保全	(2021)粤0192民初1978号[采信]	2021年3月22日	未论证

1.“法”“技”的冲突表现

有学者总结了电子数据这一证据种类自《民事诉讼法》修法以来与刑事诉讼领域对比的司法现状：使用数量上、被采信程度上、法条规范上均远低于刑事诉讼领域。同时分析认为原因在于电子证据的载体危机。[⑦]随着区块链技术应用于司法领域三四年以后，“不可篡改”“可溯源”等词汇已经为法官们所熟知，法官们的认知状态也从“完全不懂”转变为“似懂非懂”。在高企的审判压力下，法官对于区块链证据的态度也因“积极”“谨慎”“固守”的不同，在判决书中的论述分化为：“技术论证派”“不说理派”和“套话派”。具体表现为：

(1)认证趋于虚化：由于法官在技术专业领域的知识短板，使得司法实践中大量的区块链证据质证流于形式，呈现出认证过程“传统化”[⑧]和“虚化”的现象：部分案件中法院仅在查明阶段引用“存证函”的内容，在未写明理由而直接采信了电子证据[⑨]。

(2)他项转化论证：目前对区块链证据审查及采信过程说理较为详尽的代表性判决大都集中在“区块链的法律性质”论述、“取证过程可信度”审查、“区块链证据完整性”审查、“存证平台及其运营公司资质”审查上[⑩]。另有将区块链证据的“保全证书”按照《电子签名法》电子认证资质进行审查的否定性论述[⑪]；还有区块链证据按照“数据电文”对待转化，依照《中华人民共和国电子签名法》第八条审查存证平台的资质、电子数据生成及储存方法的可靠性、保持电子数据完整性方法的可靠性等方面，对涉案电子数据的效力作出肯定性认定[⑫]。

(3)论证索然寡味：这类判决“形式丰满、内容骨感”，关于平台存证的论述看似形式丰满，细读发现通篇的“套话”：“×年×月×日原告向易保全申请对……的文章进行取证保全，并形成电子数据文件。……公司出具了编号为×××的《电子数据取证证书》”[⑬]“易保全于×年×月×日对被告进行了取证保全，并作出了×××号电子数据存证证书。……上述事实，有原告提交的侵权页面取证保全文件等证据在案佐证。”[⑭]“……由第三方网络平台通过区块链技术固定、提取，且经勘验、核查属实，……本院确认其证据效力。”[⑮]

2.“法”“技”冲突的根源

产生这种现象的深层次原因与体制性障碍不无关系。法官是一个法律专家，并非全知全能的“哲学王”。[⑯]在电子证据转化为公证书存证的时代，有“国家公证”模式来转嫁司法成本。但当区块链存证到来时，电子证据的独立性价值体现则落在了法官个人身上。虽然《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11条第2款从电子数据生成存储的平台资质、取证技术和数据完整性等六项要件列明了审查判断项目，在一定程度上给出了指引，缓解了法官审查区块链证据的压力，但这实际上是将电子证据的真实性认定法律内涵转化为对存证平台的存证行为论证，又将审查方法指向另一技术领域。

在传统证据“原件标准”无法回应电子证据真实性的情况下，区块链证据的“真实性”审查亦很难得到明确的指引。在传统证据领域“真实性”一般指法律真实，而电子证据的真实性更多强调要符合技术客观和科技理性。这导致法官在判断真实性时产生障碍，当这种障碍遭遇到案件上诉率、改判率、发回重审率等考核指标时，法官们很难对区块链证据的边界进行实质性突破。再糅杂进认知不足这一因素，便导致“不说理派”和“套话派”的出现，这两派产生的根源在于“规避心理”，近三年的集中表现为从“歧视”区块链证据转向为“闭眼——一概认可”区块链证据。

二、解析原理：区块链证据何以自我鉴真

(一)“法”：真实性的二元标准

最高人民法院在《民事诉讼程序繁简分流改革试点问答口径(一)》第29个问题是“当事人提交的电子化材料有何效力”，回答是：“根据《实施办法》第二十二条，经过人民法院审核通过的电子化材料，具有‘视同原件’的效力，可以直接在诉讼中使用，但该效

力仅针对电子化材料形式真实性，对证据的实质真实性、关联性和合法性必须通过举证质证程序审查。”由此看出，司法规范性文件中明确了形式真实性与实质真实性是电子证据真实性的两层含义。形式真实性是证据资格(可采性)的判断标准，实质真实性更多偏向证明力上的标准。

这样划分有助于破解电子证据的专业性与证据采信原则之间的天然冲突。近代以来，各国基于裁判理性的考量一般实行自由心证的采证原则。我国近年所强调“注重证据之间相互印证”的也融合了一部分“心证”的合理内核。

随着科技与司法融合不断深入，电子证据的采信使得法官陷入上述体制产生的原生障碍。美国证据法学者麦考密克曾说，让法官采信科学证据就是要他做“力所不能及”的裁判。[17]大陆法系的德国证据法学者罗科信也曾说，“当用自然科学的知识可以确定事实时，此时法官的心证即无适用之余地”。[18]但当把真实性用二元标准划分后，便为法官逾越这种原生性体制障碍提供了有力抓手。

(二)“法”：真实性的三个层面

区块链证据真实性认知的障碍本质上与电子证据真实性的认证困境是同源的，恰又因区块链技术的存在和介入为破解这种障碍提供了一个特殊的途径。有学者认为，电子证据的真实性有三个层面：电子证据载体的真实性、电子证据数据的真实性、电子证据内容的真实性。[19]在司法实践中判断这三个层面的真实性，是翻越真实性认知障碍的重要途径。在讨论区块链证据是如何以其特殊技法来逾越障碍之前，先来看下现行规范对于真实性认定的路径指引。

1.载体真实的二元归属：电子证据载体的真实性可以细分为载体来源真实性和载体流转真实性。[20]

(1)载体来源真实性讨论中，我们以北京互联网法院司法区块链电子证据存证及验证流程为例(见下图1)：当事人在接入了司法区块链的第三方平台上使用电子合同、版权登记等业务，其在签订电子合

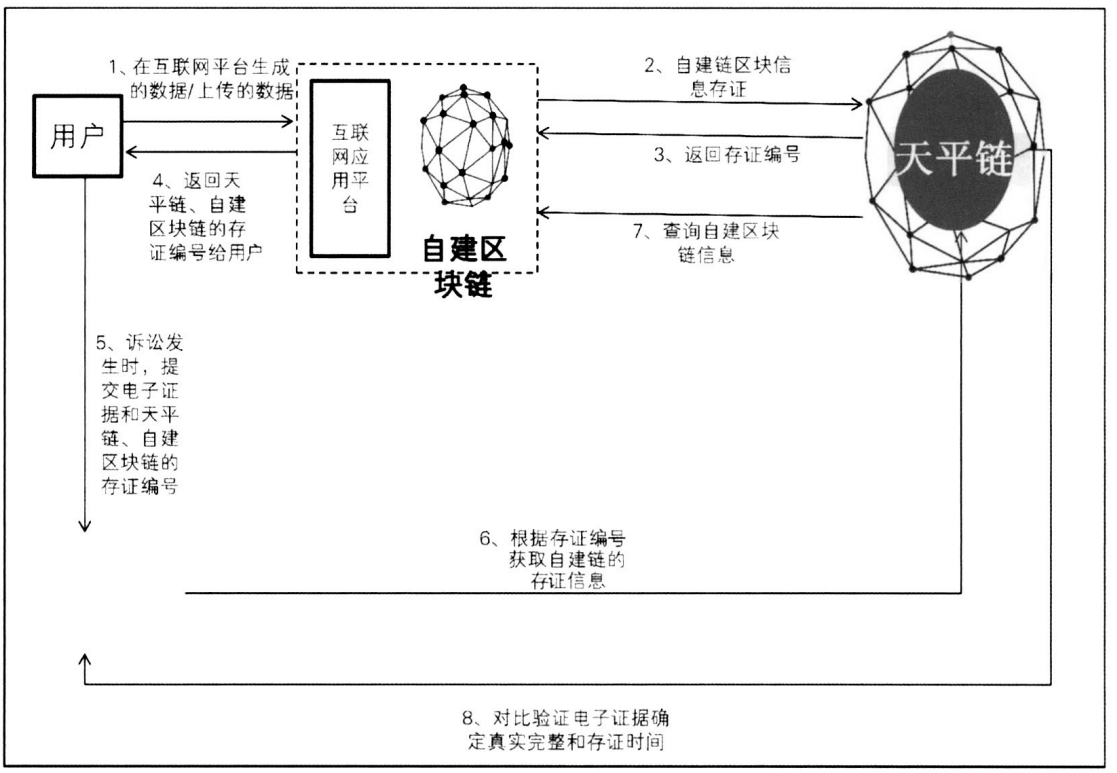

图1 司法区块链与第三方平台对接存证验证流程图

同、登记版权的时刻，数据哈希值就已经同步在司法区块链存证。此时，第三方平台和当事人获得该链返回的存证编号。当事人发生诉讼时向法院提交存证过的证据时，同时提交对应编号文件，司法区块链后台自动解析存证时的哈希值进行对比，如果哈希值相同，该数据没有被篡改即验证成功，如果二者哈希值不同，则意味着其被篡改过，并将上链标识、区块链验证状态、存证时间、存证内容、验证成功/失败等信息推动给法官，从而辅助法官判案，提升法官对于电子证据的采信效率。

不难看出，原生区块链证据的载体来源真实性是有区块链系统来保证的；而非原生(当事人上传)的区块链证据其载体来源真实性是由上传前的载体来保证。

(2)对载体流转真实性的讨论，我们可以借鉴香农在《通信的数学原理》中提出信息论的基本论点——形式化假说(即，通信的任务只是在接收端把发送端发出的消息从形式上复制出来，消息的语义、语用是接收者自己的事，与传送消息的通信系统无关)。“形式化假说”对区块链系统存证同样适用：区块链保证了电子证据一旦写入，就全网可见、不可篡改。[21]可见，不论原生区块链证据还是非原生区块链证据其载体流转真实性都是由区块链技术保证的，本文作者称之为“区块链形式化假说”。所以，载体流转真实性应属于电子证据形式真实性层面的问题。

2.数据真实的二元归属：基于区块链不可篡改[22]的技术特征，如果区块链外数据在源头和写入环节能够保证真实准确，那么写入区块链内的电子证据就意味着数据未被篡改。从这点来看，区块链系统虽然没有提升数据的真实准确性，但却能够保证电子证据的哈希值在封装进相应区块后不会改变，从而确保了电子证据的数据同一性和数据完整性。可见，区块链技术存证这一特殊的电子证据固证方式使得电子证据的数据真实完全由技术来保障完成，因此也是形式真实性层面的问题。

3.内容真实的二元归属：区块链证据能否与其他证据形成印证关系、能否反映与案件相关的法律事实等问题都不是区块链系统所能够保障的，因此区块链证据内容真实性应属于电子证据实质真实性层面问题。需要拆解说明的是，“实质真实性”中蕴含了关联性的部分内容。证据必然是由“载体”[23]承载了反应案件的信息，而电子证据中的“信息”又可以分为数据和内容。“数据”更多需要客观认定是否真实，可以如同上文在真实性范畴讨论；“内容”更加需要结合案情进行关联性认定，因此“内容真实”无法由区块链系统保障。这点上与传统证据审查是无异的，而“关联性”并非本论文讨论的重点。

有学者曾提出“只要法律承认区块链技术的合法性(或不禁止区块链技术的社会化应用)，那么基于区块链技术所提供的证明就具备证据的合法性要件”[24]。本论文作者认为这一论断改为“只要法律不禁止区块链技术的社会化应用，那么基于区块链技术固定的电子证据就具备了形式真实性的合法要件”更为恰当。

(三)“技”：五技法成就自我鉴真能力

我国司法实践通常所说的“证据相互印证”，是指两个以上的证据所包含的事实信息得到相互验证的状态。[25]这种证据相互印证的观点是司法实践长期的一种经验总结。从刘品新老师在《论电子证据的真实性标准》一文中所进行的田野调查结果来看，电子证据通常是通过与其他证据组合的方式而被采信，这也符合“证据印证”这一司法认知惯性。印证体系的证明方法具有以下特点：“证据的多数性”“可重复检验的特性”“客观性”和“稳定性”。[26]而区块链证据这一特殊的电子证据存证形式，因为借助了区块链系统进行数据固定，因此天然具备了系统性。这种系统性的天然存在几乎完美的覆盖了印证体系的上述四个特点。

1.区块链证据的多数性和载体内部可印证性

孤证不能作为定案依据是印证模式的基础，即必须有两个以上不同来源的证据，它们之间环环相

扣共同指向一个事实。相较于传统证据及其他电子证据，区块链证据会让同一行为在不同节点留下相关的数据簇，这些数据簇之间是依据约定的决策机制自动达成共识[27]，共享同一份数据。

具体来说，是以区块为单位的链状数据块结构：区块链系统各节点通过一定的共识机制选取具有打包交易权限的区块节点，该节点需要将新区块的前一个区块的哈希值、当前时间戳、一段时间内发生的有效交易及其梅克尔树根值等内容打包成一个区块，向全网广播。

这种全网广播的数据簇中的数据之间虽然是传来取得，但是因为有了算法保证，可以在转递过程中不失真(无损传递)，且在执行算法过程中会同步生成一些附属信息(如创建、修改、访问的时间、制作人、路径、临时文件等)及关联痕迹(数据文件、数据流文件、临时文件等)，这些都从印证理论上使得区块链证据形成了印证模式的“内部证据链”自洽状态。

2.区块链证据的可重复检验性

(1)可重复检验性的宏观层面，可以通过“蓝牛仔公司与华创汇才公司侵害作品信息网络传播权一案”[28]进行说明：其一，蓝牛仔公司之前曾向版权家(第三方存证平台)申请被侵权证据电子数据存证，并获得版权家电子数据存证证书，经版权家可信存证系统进行保管。版权链通过跨链操作将版权链区块的摘要数据在“天平链”上存证，“天平链”返回给版权链一个天平链存证编号，版权链再返回给用户一个包含在天平链上的存证编号以及在版权链上的存证编号的文件。其二，通过版权大数据监测，发现本案中涉及的原告在其平台上存证的电子数据被侵权，即收集相关的侵权图片线索，将侵权线索存证上版权链，版权链通过跨链操作将版权链区块的摘要数据在天平链上存证，“天平链”返回给版权链一个天平链存证编号，版权链再返回给用户一个包含在天平链上的存证编号以及在版权链上的存证编号的文件。其三，当诉讼发生时，原告蓝牛仔公司通过北京互联网法院电子诉讼平台进行网上立案，同时提交起诉状、用户身份验证信息、确权存证原文件、侵权线索原文件及包含区块链存证编号的文件。北京互联网法院电子诉讼平台调取天平链进行自动验证，验证结果显示涉案证据自存证到天平链上后，未被篡改过，得出区块链存证“验证成功”的结果。

(2)可重复检验性的微观层面，是由哈希值[29]来保证的：每份电子证据(数据)经由哈希算法[30]计算得出的数据指纹都是唯一的，只有相同的输入数据经哈希算法计算后的结果输出才是同一的。由此保证了微观层面的可重复检验。

3.区块链证据的客观性

区块链证据的客观性主要体现在防篡改的“技术”上：链式结构中的哈希算法和分布记账融入链式结构中。

数学计算，哈希算法应用于链式结构产生客观性：在区块链中，每个新区块都包含上一个区块经过科学方法算出来的数据指纹——哈希值。这个值让一个个区块之间形成了有着严格顺序关系的链条结构，一旦某个区块中的任何数据被篡改，该区块在下一个区块头部的数据指纹(哈希值)就会变动，后续所有区块的数据指纹(哈希值)都会变动，所有人都能发现数据被篡改，并丢弃且不认可这种无效数据。这就保证了区块链数据的不可篡改。

结构方式，分布记账融入链式结构产生客观性：在区块链系统中，根据一套竞争规则，选出记账人(节点)，参与竞争的人都有机会获胜当选记账人(节点)。[31]一次记账完成，就是一个新区块被挖出，这个区块信息是固定的，它有自己独有的数据指纹(哈希值)[32]。在下一轮记账中，新的节点记录新一页账单(挖出新区块)，新的账单的头部(区块头)需要记录上一页账单的数据指纹(上个区块的哈希值)，这就保证上一页账单和当前账单建立有明确顺序的紧密关联。若上一页账单数据被修改，那它的数据指纹(哈希值)会发生改变，就无法与下一页账单中记录的哈希值对应上。所有链上节点就能识别出这是个被篡改的无效链，并将其抛弃。而上个区块的头部也记

录了上上个区块的哈希值，这样整个区块链环环相扣，有严格的先后顺序，且只要某个区块数据被篡改，其后所有区块的记账数据就会发生改变，可谓“牵一发而动全身”。这就是区块链记账的第三大特点：链上所有区块，环环相扣，通过算法保证全链信息无法篡改。

4.区块链证据的稳定性

稳定性寓于区块链溯源中：加入区块链中的记录被永久存储，区块链的链式结构，使得即使在某时某刻发生了变更，也会被完整记录，这样就可以追溯到发生变更的区块(从而定位到修改的时间和位置)，从而保证不可被篡改。区块链的特点使得“作恶”的成本大为增加，从而使得没有人(节点)会去作恶。

以天平链为例客观性与稳定性体现在：基于天平链的数据哈希存证的业务特点以及天平链各节点安全管理的现状，同时考虑到效率问题，当前配置的是基于Kafka的高速共识算法[33]。共识分为三个阶段：背书阶段、排序阶段和验证阶段。该算法对总节点数没有特定要求，能容忍半数以下节点发生故障。背书节点对交易请求包背书(签名)、排序服务对被认可的交易进行排序，确保交易顺序的一致性、记账节点获取有序事务块并验证其结果的正确性，包括检查背书策略和重复提交攻击。

5.区块链证据的痕迹可补强性

区块链的分布式结构，是通过点对点通信技术，实现各主体间点对点的信息传输。由于每一个区块都是与前续区块通过密码学证明的方式链接在一起的，当区块链达到一定的长度后，要修改某个历史区块中的交易内容就必须将该区块之前的所有区块的交易记录及密码学证明进行重构，这不但从技术上加大了篡改成本，进而有效实现了防篡改，同时还使得痕迹得到补强。

以天平链为例，是采用基于账户的数据记录方式，基于账户的数据模型可以更方便的记录、查询账户相关信息。而三种账本——区块账本[34]、状态账本[35]和历史账本[36]使得区块链证据在印证体系下能够自我痕迹补强。

通过以上分析可以看出，区块链证据在印证证明体系下具备自我鉴真的技术能力。

三、认定路径：规则运用及完善

(一)区块链证据的原件属性获得

综观当今世界，对电子证据原件的理论认知和立法例实践主要有：功能等同法、拟制原件说、混合标准说、复式原件说、结合打印说。[37]这五种学说发端于不同类型的电子证据，在各自的领域都有恰当的切入点，但很难普适于当下全类别电子证据。单就区块链电子证据来说，笔者认为能够非常恰当契合适用的是复式原件说以及混合标准说[38]的理论原理内核。

1.微观节点间的复式原件属性：区块链的分布式结构和通过点对点通信技术实现各节点间信息传输的技术特性，使得数据几乎在同一时间传遍全链各个节点。从各个节点的数据来看，难以分辨谁是“原件”谁是“复本”；而分布结构的传输路径，使得难以区分哪个节点是“原始取得”哪个节点是“传来取得”。这种特性像极了司法实践中当事人签订合同时往往制作同一内容的一式二份，分别签字盖章后双方各执一份的“复式原件”[39]。可见，如果区块链证据从区块链节点作为微观切入观察，不难发现各个节点上的数据均具备“复式原件”的属性。借由此，区块链证据在跳出微观观察后，整体对外获得了一种可自我鉴真的原件属性。

2.宏观系统上的复式原件属性：如果以区块链系统宏观作为一个整体看待，对其存储的数据直接证明完整性和准确性难度是非常大的，因此可以考虑从计算机服务器的系统可靠性来替代数据记录的可靠性，以此来完成检验完整性和准确性的任务。如果直接源于区块链系统的数据能够作为一个“整体物”而精准输出[40]，那么这种“精准输出物”即为数据原件。必须强调的是，这句看似与“拟制原件说”相同的结论的前提是区块链系统的可靠性，而这个

可靠性是由宏观层面国家标准或行业标准认定的符合存证要求的区块链系统来保证的。

(二)“3+2”鉴真范式

同是法条独立的情况下,对比刑事诉讼,绝大多数裁判文书在对电子证据的形态和取证过程描述后,最终都采信了该电子证据。[41]参考刑事诉讼领域证据认定路径,类比民事诉讼领域,区块链证据以法庭示证为分水岭认定路径总结为“3+2模式”。

1.“3”:存证三方面标准建设:存储方法“合法”性、存储程序合法性、证据表现合法性。

(1)正面主体:存储方法“合法”[42]认定条件

在现行法律未对区块链存证平台设定准入门槛的情况下,区块链证据鉴真首先需要考察的是平台提供的存证技术方法的合法性。具体来说:

①存证平台安全应从以下6个层面考察[43]:系统安全、运行环境安全、存储安全、通信网络安全、数据安全、系统软件安全。

②存证数据应满足双“可”:数据可追溯、时间可信。如前所述,数据可追溯是区块链证据可重复检验性的技术基础,是客观性的技术保障。时间可信是指时间戳应唯一地标识某一刻时间的字符序列,该标识不仅可以标识出行为的发生时间,还可以通过时间的先后顺序构建带时序的证据链条。这是区块链证据通过技术在印证理论下实现的自我鉴真。

③数据存证服务提供者应记录过程时存证平台自身的硬件设备信息、软件系统信息、网络信息及存证过程数据等,同时计算这些信息的完整性校验值,并将记录的数据与对应的完整性校验值同时进行存证。

(2)侧面过程:存储程序的合法认定条件

存证平台提供了可靠的技术和稳定运行的系统后,还应考察当事人(即存证服务使用者)在具体操作过程中的程序正当性:

①电子数据存证前,存证平台应对使用者进行身份核验。电子证据存证服务使用者应检查存证行为实施的计算机系统的软硬件及网络环境是否安全可靠且处于正常运行状态,存证平台可以将这些信息也进行存证,以增加证据链上的多节点印证自洽丰满度。

②电子数据存证时,电子数据存证服务使用者使用电子证据存证服务提供者提供的应用程序、网站等,应将数据原文或完整性校验值及其附属信息等数据同步传至电子数据存证平台。

(3)传输及示证过程:表现形式合法

存证后存证服务使用者需要提取存证标识码等或在举证示证阶段需要验证时应在两个条件进行考察:

①身份认证:数据存证平台应在使用者传输数据前对其身份进行可信认证,并保留认证记录。

②传输完整性:应采用校验技术对传输数据进行校验,确保传输数据的完整性。

2.“2”:六维示证及翻越“内心确认”门槛

(1)“示证-验证”6维度

存证平台至少应提供6个维度的验证结果以保证形式真实:存证标识码、数据原文(或原文完整性校验值及校验算法)、时间标识、当事人信息、存证日志信息、其他附属信息。

(2)翻越“内心确认”的门槛

“技证真实”的逻辑是通过“保留事实”以便再次呈现,所以电子证据生成、存储、传输所依赖的区块链软硬件系统的完整性和可靠性以及实现“保留”动作时系统否处于正常运行状态就成为区块链证据呈现形式真实性的关键所在。按照数据[44]的生成、收集、存储、传输、提取全生命周期结合前述的“条件”来分析:

①生成上链时间节点:电子证据原生于链上还是链外生成后再上链,是否需要适用前文论述的“区块链形式化假说”的前提。原生于链上的数据是生成即上链,这集成了电子证据生成和收集两个环节。链外数据上链要考察数据上链后生成和存储分别考虑。在存储环节可以考虑适用“校验值验证”方法来判断真实性,即:电子证据通过公认技术

手段得到了完整性校验就足以验证真实性。换言之，使用特定算法对该电子证据的不同版本进行计算得出的哈希值一致，则视为链上的副本与原本相同[45]。但不论电子证据属于那种上链形式，考察区块链系统的可靠性都应满足本节的“方法合法”和“程序合法”条件。

②区块链系统的可靠性认定：当区块链系统满足一定标准后即存储于其上的电子证据就得到了由该系统产生的、经证实的推定性[46]真实。这种真实性标准在美国《联邦证据规则(2017年)》902(13)中被称为“电子记录验证”标准，具体译文为：下列品目的证据是自我鉴真的证据，无须提供外在的鉴真证据即可采纳：……(13)由电子程序或系统产生的、经证实的记录。由电子程序或系统产生的记录，该电子程序或系统经由符合规则902(11)、(12)要求合格人员证实能产生准确的结果。[47]

落到实践操作层面，电子证据生成、存储、传输三个环节统一要考察区块链系统在系统技术指标、数据传输方式和加密校验方式上至少应符合《电子数据存证技术规范》[48]。当区块链系统符合该技术规范，可以认为区块链系统的软硬件环境具备有效地防止出错的监测和核查手段，并且可以认为区块链系统保存、传输、提取电子证据的方法可靠。

(三)“区块链形式化假说”的补强方法

当“区块链形式化假说”失效时，应当允许当事人对区块链证据进行补强。

1.鉴定补强：《人民法院在线诉讼规则》第19条在吸收《互联网法院审理案件若干问题的规定》第11条合理内核基础上直接将“鉴定”扩展到区块链证据鉴真上。

2.印证补强：《人民法院在线诉讼规则》第18条否定性的指明无法印证补强的后果，而第19条从正面指引可以通过“调取其他相关证据进行核对”进行印证不强。这两条可以称为“区块链证据补强专条”，并进一步细化，当程序合法条件不满足时，并不必然导致真实性丧失，可以通过以下三个途径进行印证证明体系的补强：(1)说明上链存证数据的具体来源、生成机制、存储过程等情况；(2)提交公证或第三方见证的其他关联印证数据来佐证真实性；(3)上链数据是在正常的往来活动中形成和存储。

(四)结论：鉴真的实践迈进

电子证据的生成、存储、传输三个环节满足上述“3+2”范式后，可以认为区块链系统的系统技术指标、数据传输方式和加密校验方式上已经满足《人民法院在线诉讼规则》第17条要求的“国家标准或行业标准”，即：该区块链证据使用的区块链系统软硬件环境具备有效地防止出错的监测和核查手段，同时存储电子证据的行为和方法可靠，该区块链证据上链后未经篡改，具备真实性。

四、结语

党的十九大报告指出，建设现代化的社会治理能力需要构建“共治、共建、共享”的社会治理新格局。区块链技术本身是在一个数字世界里围绕着数据的记录、组织和传播的一种共建、共享、共治的新技术。按照新兴技术的发展规律，当一个高端科技推进人类文明的发展进程时，它最需要关注的问题不是该技术本身所达到的高度，而是该技术如何影响其他技术的革新，从而推进人类文明的整体提升。[49]随着《最高人民法院关于互联网法院审理案件若干问题的规定》《最高人民法院〈关于民事诉讼证据的若干规定〉》《人民法院在线诉讼规则》等司法解释对区块链证据亮明了司法态度和司法实践对科技接纳的变化，这种存证手段已经从互联网审判走向了传统法院的针对电子证据的普适存证手段。法学界和司法实务界均意识到，反复讨论区块链技术监管无助于推进科技与现代法治的有机融合。学界和实务界都应该以动态、体系化的视角来全面审视区块链技术的理发定位、行政规制与司法裁判的问题。区块链证据真实性的二元划分法有助于改变过度集中关注区块链证据依托的科技载体的可信度，从而可以提升司法效率和压缩司法成本。同时，有助于防止法官陷入“一切皆可造假”的哲学思辨中，

扭转受传统诉讼法学和证据法学理论影响而产生的查明事实真相绝对化的思维定式。须强调，虽然在最高法院的司法文件中涉及了“形式真实性”“实质真实性”的提法，但法律和司法解释层面并未规定这两类的审查原则。作者认为，在证据审查过程中，引入需要补强证据规则，不但可以防范区块链证据“偏在”于具有技术优势的一方，同时可以在法官内心形成事实上的确认，有助于法官在判决中更好的明示心证形成过程，最终将二元标准在现行法律框架下实现“合二为一”的真实性审查。在对区块链技术尚未出台相应立法层面规范的情况下，区块链证据的司法审判规则探讨或许能够给我们带来技术与司法碰撞后的进一步推进与更深层次的融合。

注释：

①我国法律中主要使用“电子数据”一词，域外法律中主要使用“电子证据”一词，两者词义基本同一。本文统一使用“电子证据”，在引用时遵从原文表述。

②本文中后续将使用“区块链证据”一词指代通过区块链技术手段固定的电子证据。

③调研以问卷发放和举办座谈的形式与字节跳动公司、滴滴公司、腾讯公司、安妮股份主体等进行沟通交流，了解当前中关村企业对于区块链技术运用的需求和知识产权保护方面的需求，问题包括：在保护知识产权方面是否有使用区块链的需求、使用区块链的需求是什么、在保护知识产权方面是否有自行建设区块链的需求、在维权诉讼中，取证首选的方式是什么。

④为了能够更好地观察纠纷类别，此处将案由细化到二级案由和三级案由。

⑤2019年6月有研究者因样本不足，通过在中国裁判文书网民事裁判文书项下以“IP360、易保全、美亚柏科、存证云、保全网“等平台名称检索的方式获取样本。时至今日，论文作者发现以“区块链”为关键词检索获得的样本已经足够研究使用。

⑥裁判文书网显示2010年有一份“区块链”文书，打开后案号为(2019)粤0304民初26964号，该判决为2019年作出。

⑦参见刘哲玮：《民事电子证据：从法条独立到实质独立》，载《证据科学》2015年第6期。

⑧这里指按照传统证据的认证规则进行认证。

⑨(2021)闽01民终1542号民事判决书、(2021)苏0591民初712号民事判决书。

⑩杭州互联网法院(2018)浙0192民初81号民事判决书，北京市东城区人民法院(2018)京0101民初4624号民事判决书，四川省成都市中级人民法院(2019)川01民终1050号民事判决书。

⑪(2019)川01民终1050号民事判决书。

⑫(2018)京73民终2163号民事判决书。

⑬(2019)闽01民初436号民事判决书。

⑭(2019)豫05民初29号民事判决书。

⑮(2019)鄂01民初4408号民事判决书。

⑯参加柏拉图：《理想国》，郭斌和、张竹明译，商务印书馆2012年版，第217页。

⑰参见[美]约翰·W.斯特龙、麦考密克：《麦考密克论证据》，汤维建等译，中国政法大学出版社2004年版，第400页。

⑱[德]克劳思·罗科信：《刑事诉讼法》，吴丽琪译，法律出版社2003年版，第121页。

⑲参见褚福民《电子证据真实性的三个层面——以刑事诉讼为例的分析》，载《法学研究》2018年第4期。

⑳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。

㉑伊然、董学敏：《互联网审判中区块链存证技术应用进路研究》，载《人民司法》2020年第31期。

㉒不可篡改的特性主要由时间戳和加密算法来保证。

㉓参见陈瑞华：《刑事证据法学》，北京大学出版社2012年版，第63页：所谓“证据载体”，是指那些记载或者证明一定证据事实的证据形式。

㉔张玉洁：《区块链技术的司法适用、体系难题与证据法革新》，载《东方法学》2019第3期。

㉕陈瑞华：《论证据相互印证规则》，载《法商研究》2012年第1期。

㉖参见谢小剑：《我国刑事诉讼相互印证的证明模式》，载《现代法学》2004年第6期。

㉗目前区块链技术的共识算法主要有工作量证明(PoW)、权益证明(PoS)、股份授权证明(DPoS)、拜占庭容错机制(PBFT)。

㉘2014年5月10月，蓝牛仔公司发表一幅名为“快乐的年轻人玩手机和电脑”的图片。2015年12月28日，根据申请，北京市版权局颁发京作登字-2015-G-00625457号《作品登记证

书》,将包括涉案照片在内的摄影作品的著作权人登记为蓝牛仔公司。微信公众号华创资本(China Growth Capital)为华创汇才公司开办。2017年4月20日,在被告华创汇才合作公司的要求下,由被告合作公司提供稿件,华创资本公众号内发表一篇名为《在帮中国人炒美股这件事上,为什么老虎证券走在了前头》的文章。文章中使用了涉案图片。故原告蓝牛仔公司要求被告华创汇才公司赔偿损失及合理费用。

㉙哈希值又译作:散列值、哈希散列值。

㉚哈希算法也叫散列算法或者数据摘要,其原理是将一段信息转换成一个固定长度并具备以下特点的字符串:(1)如果某两段信息是相同的,那么字符也是相同的;(2)即使两段信息十分相似,但只要是不同的,那么字符串将会十分杂乱随机并且两个字符串之间完全没有关联。本质上,哈希算法的目的不是为了"加密"而是为了抽取"数据特征",也可以把给定数据的散列值理解为该数据的"指纹信息"。典型的散列算法有MD5、SHA1/SHA256和SM3。

㉛"中本聪"设计方法是,谁最先做出数学题的答案,谁就获得记账权。这体现了区块链记账的一个特点:非中心化记账。通过做题随机产生记账人,保证记账人不再是某个中心化机构。每一次数学解题竞赛中,都只产生一名获胜者,由他来进行记账,记账信息打包生成一个数据包,该数据包称为区块(即挖出一个新区块)。其他玩家验证无误后,将这个新区块复制(下载同步)到自己维护的区块链上,这就保证了所有玩家虽是分布式记账,但所有人的账本数据是一致的(区块链上信息相同)。这体现了区块链记账的第二大特点,所有节点维护的账本一样,对账非常方便。

㉜通过对该区块进行哈希运算,产生该区块的哈希值,该区块发生任何变化,区块的哈希值就会有巨大改变。这样也就保障"不可篡改性"。

㉝即基于Zookeeper(分布式服务框架)的Apache Kafka(分布式消息系统)的共识。

㉞区块账本:记录智能合约的交易记录,保存在文件中。

㉟状态账本:保存智能合约数据的最新状态,保存在KV(Key-Value)数据库中。

㊱历史账本:保存所有智能合约执行交易的历史记录索引,保存在KV数据库中。

㊲刘品新:《论电子证据的原件理论》,载《法律科学(西北政法大学学报)》2009年第5期。

㊳这一学说实际上是采纳了"功能等同法"和"拟制原件说"在各自适用领域的长处形成的一套新的原件理论。典型代表立法例是:加拿大统一州法委员颁布的《1998年统一电子证据法》第4条。

㊴本文作者按:复式原件说的立法例是菲律宾《电子证据规则》第4条第2款:"……如果某一文件在同一时刻或前后不久就同一内容执行两份或更多复本,或者该文件是通过与原件相同的印模、或者使用同一字模、或者通过机械或者电子的再录制或者通过化学复制方法,或者通过其他能正确复制原件的相应技术而形成的复制件,则对该复本或复制件均应视为原件的相当物"。

㊵本文作者按:美国法上所说的"精准输出物"立法例为:《联邦证据规则》1001(3)、《1999年统一证据规则》1001(3)、《加利福尼亚州证据法典》第255条。

㊶刘哲玮:《民事电子证据:从法条独立到实质独立》,载《证据科学》2015年第6期。

㊷这里的"合法"主要指符合技术规范和理性的真实观。

㊸具体技术安全标准规范参照《电子数据存证技术规范》(SF/T0076-2020)。

㊹此处区分"数据"与"电子证据"概念外延,即数据大于电子证据,以数据上链后划入电子证据范畴。

㊺这种做法可以从2017年美国《联邦证据规则》902(14)中找到立法例,该法允许通过提交"从电子设备、存储介质或文件复制而来的、经证实的数据"进行鉴真。"经证实"指复制同时哈希算法得出的哈希值。

㊻这种推定并不是法律推定标准的体现,而是"信息系统完整性"标准的体现,即:通过可靠信息系统产生的电子证据推定属实,立法例为《加拿大1998年统一电子证据法》(Uniform Electronic Evidence Act(1998),sec. 4)。

㊼参见Fed. R. Evid. 902(13)。

㊽司法部于2020面5月29日发布和实施,属司法行政行业标准。

㊾参见陈立洋:《区块链研究的法学反思:基于知识工程的视角》,载《东方法学》2018年第3期。