区块链技术下数据存证的法律效力研究

郭明轩
（沈阳工业大学　文法学院，辽宁　沈阳　110870）

摘　要：传统证据“三性”的审查框架在应对电子数据存证时面临信任危机，区块链技术为破解困境提供了新的路径。其通过哈希校验、链式结构与分布式存储确保数据上链后不可篡改，并在我国司法实践中被明确为电子数据的特殊固定方式，获得推定真实的法律地位。然而，技术信任无法直接等同于法律真实，区块链存证仍面临上链前数据真实性悖论、举证责任分配失衡、隐私保护与永久存证冲突等核心挑战。通过比较中外规制路径可见，需超越传统证据属性论的局限，构建分层动态的全链路审查体系，此体系应融合技术自证与司法核验，依据存证类型细化举证责任，并推动标准统一与链间互通，从而将区块链存证的审查纳入科学化、规范化的轨道，以达至司法公正的诉讼目标。

关键词：区块链技术；电子证据；证据审查；法律真实
中图分类号：D916.3；D915.13；TP301.6　　**文献标志码：**A　　DOI：10.19358/j.issn.2097-1788.2026.07.008

中文引用格式：郭明轩. 区块链技术下数据存证的法律效力研究[J]. 网络安全与数据治理，2026，45(7)：55-61.
英文引用格式：Guo Mingxuan. A study on the legal effect of data evidence preservation under blockchain technology[J]. Cyber Security and Data Governance，2026，45(7)：55-61.

A study on the legal effect of data evidence preservation under blockchain technology

Guo Mingxuan
（School of Humanities and Law，Shenyang University of Technology，Shenyang 110870，China）

Abstract：The traditional review framework of the "three attributes" of evidence is confronted with a credibility crisis when dealing with electronic data evidence preservation，and blockchain technology provides a new path to break through this dilemma. By virtue of hash verification，chain structure and distributed storage，it ensures that data cannot be tampered with after being uploaded to the blockchain. In China's judicial practice，it has been explicitly defined as a special method for fixing electronic data，and has obtained the legal status of presumed authenticity. However，technical trust cannot be directly equated with legal authenticity. Blockchain-based evidence preservation still faces core challenges such as the authenticity paradox of data before being uploaded to the blockchain，the unbalanced allocation of burden of proof，and the conflict between privacy protection and permanent evidence preservation. A comparative study of Chinese and foreign regulatory approaches shows that it is necessary to transcend the limitations of the traditional theory of evidence attributes and construct a hierarchical and dynamic full-link review system. This system should integrate technical self-certification and judicial verification，refine the burden of proof according to the types of evidence preservation，and promote the unification of standards and interoperability between blockchains. In this way，the review of blockchain-based evidence preservation can be brought into a scientific and standardized track，so as to achieve the litigation goal of judicial justice.

Key words：blockchain technology；electronic evidence；evidence review；legal authenticity

0　引言

当前，第四次工业革命正以前所未有的深度与广度重塑社会形态。社会生活的全面数字化使得电子数据取代了传统的纸质载体，成为还原客观事实的核心媒介。然而，这一变革同时也带来了前所未有的信任危机。

电子数据具有无形性、易篡改性、易伪造性以及对存储环境的高度依赖性等先天缺陷。在司法实践中，如何证明一份电子合同未被单方修改？如何确认一张网页截图生成于特定的历史时刻？如何确信服务器日

志未被管理员后台覆写？这些鉴真难题长期困扰着法官与当事人，导致了极高的取证成本与极低的司法效率。传统的公证取证虽然效力较高，但其高昂的时间与金钱成本难以适应互联网时代海量、高频、碎片的纠纷特征。

区块链技术的出现，为解决这一信任难题提供了一把“技术钥匙”。作为一种去中心化、不可篡改、全程留痕的分布式账本技术，区块链被《经济学人》誉为“信任机器”。自 2008 年中本聪发布比特币白皮书以来，区块链技术迅速溢出金融领域，在司法存证、知识产权保护、供应链管理等场景落地生根。特别是在我国，随着 2018 年《最高人民法院关于互联网法院审理案件若干问题的规定》的出台，区块链存证的法律地位首次得到确认，标志着司法领域区块链证据元年的开启。

尽管区块链存证在司法实践中已呈燎原之势，但在法学理论与制度构建层面，仍存在诸多未竟之问。技术的确定性并不能直接等同于法律的真实性，区块链虽然能通过哈希校验保证数据上链后的完整性，却无法自动解决数据上链前的真实性问题，即著名的预言机问题[1]。此外，区块链存证的广泛应用还引发了隐私保护与不可篡改性的冲突、技术不对等导致的举证责任分配失衡，以及算法黑箱带来的司法审查困境。基于此，对区块链技术下数据存证法律效力的研究，亟需超越早期阶段的政策宣示、制度注疏与简单的技术应用倡导，深入技术的底层逻辑，结合国内外最新判例与学说，探讨如何构建一套既适应技术特性又符合证据法基本原理的审查规则体系。

1 区块链存证的技术逻辑与法律属性

要准确界定区块链存证的法律效力，首先必须解构其技术黑箱，理解其获得“信任”的底层机理，并在现行证据法体系中为其寻找准确的定位。

1.1 区块链存证的技术机理

哈希算法是区块链存证的基石，它通过特定的数学公式，将任意长度的输入数据转换为固定长度的输出字符串，即哈希值。这一过程具有两个关键特性：第一，单向性。在现有计算能力下，无法从输出的哈希值逆向推导出原始电子数据的内容。这一特性在存证结构中具有双重意义，既实现了底层原始数据的隐私隔离，又满足了证据固定过程中的保密性要求。第二，抗碰撞性。原始数据的任何微小改动都会导致计算出的哈希值产生翻天覆地的变化。在司法存证中，这一特性被用于校验数据的完整性。当事人将原始数据的哈希值上传至区块链，一旦发生纠纷，只需重新计算手中持有的原始数据哈希值并与链上记录比对，若两者一致，即可在数学概率上排除数据被篡改的可能性[2]。

区块链采用“区块+链”的结构存储数据，每个新区块都包含前一个区块的哈希值，从而形成一条按时间顺序严格排列的链条，每个区块在生成时都会被打上全网公认的时间戳，这为电子数据提供了不可辩驳的存在性证明。它不仅证明了数据是什么，还证明了数据在何时已经存在，这对于知识产权确权和电子合同生效时间的认定至关重要[3]。要修改链上的某个历史数据，攻击者必须同时修改该区块及其之后所有区块的哈希值，这在计算力上几乎是不可能的。

传统的电子存证依赖于单一的中心化机构，一旦该中心被黑客攻击或内部人员作恶，数据安全性将无法保障。区块链采用分布式账本技术，数据被同步存储在网络中的成百上千个节点上。在我国的司法实践中，主要采用的是联盟链架构，如司法链、天平链。这些链的节点通常由法院、公证处、司法鉴定中心、大型科技公司等具有公信力的机构共同维护，数据必须经过多方节点的共识机制确认才能上链。这种多中心的背书机制，使得单方篡改数据的成本极高且极易被发现[4]，从而实现了证据信任机制从“机构信任”向“算法信任”的范式跃迁。

1.2 区块链存证的法律定性

在我国《民事诉讼法》规定的法定证据种类中，区块链存证究竟属于哪一类，这直接关系到后续的审查规则。

2012 年修订的《民事诉讼法》首次将电子数据增设为独立的证据种类。2018 年最高人民法院《关于互联网法院审理案件若干问题的规定》第十一条明确指出：“当事人提交的电子数据，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……能够证明其真实性的，互联网法院应当确认。”这一规定在规范层面终结了关于区块链存证属性的争议：区块链存证本质上属于电子数据。它不是一种新的证据种类，而是电子数据的一种特殊的收集、固定和存储方式。

传统证据法高度强调原件优先规则，然而，电子数据的可复制性使得原件概念变得模糊。在区块链技术下，这一概念发生了更深层次的异化。施鹏鹏等指出，在区块链技术的支持下，电子数据究竟是原生证据还是派生证据显得并不重要，因为副本与原件具有

同等的可信度[5]。由于区块链上的数据是全网同步的，任何一个节点上的数据副本在数学层面都与原件完全一致。因此，司法实践倾向于认为，只要能通过区块链哈希校验的电子数据，即视为具备了原件的法律效力，或者说满足了形式上的真实性要求。

1.3 区块链存证的司法实践

我国在区块链存证的司法应用方面走在世界前列，形成了一套独特的司法与科技相结合的治理模式。这一过程经历了从法官个案探索到最高司法机关制定统一规则的演进路径。

2018 年 6 月，杭州互联网法院审理的华泰一媒诉道同公司侵权案被誉为“区块链存证第一案”[6]。法院并未因为技术的新颖性而直接排斥，而是确立了开放、中立的技术审查标准。判决书详细分析了存证平台的技术路径、服务器日志、源码识别过程，并确认了比特币区块链的不可篡改特性。法院最终认定只要电子数据来源真实、存储可靠、内容完整且未被篡改，就应当认可其法律效力。该案确立了区块链电子证据审查的个案分析法，即重点审查存证平台的资质、技术可靠性及电子数据的生成环境，有效消解了司法人员对新技术的认知壁垒与适用顾虑。

如果说杭州首案是利用公有链进行存证，北京互联网法院则开启了司法联盟链的新阶段。北京互联网法院主导建立了天平链，将法院、公证处、司法鉴定中心、大型互联网平台纳入节点。截至 2024 年，北京互联网法院天平链上链数据已超过数千万条。这种内嵌式存证极大简化了法庭质证环节，使得验证过程从数小时缩短至数秒，显著地提升了司法效率[7]。

1.4 区块链存证的立法现状

随着实践的深入，最高人民法院通过一系列司法解释和规范性文件，将区块链存证的效力认定规则化、制度化。

《最高人民法院关于互联网法院审理案件若干问题的规定》是区块链证据效力的“出生证”。其第十一条明确了法院应当对通过区块链等技术手段固定的电子数据进行审查，并确立了真实性为审查核心。这一条款解决了早期司法实践中法官因法无明文规定而不敢认证的困境，赋予了区块链技术在司法领域的合法身份。

2021 年发布的《人民法院在线诉讼规则》标志着区块链证据规则的成熟，其中第十六条至第十九条构建了区块链存证的推定效力规则，这是证据法上的重大突破。规则第十六条规定，当事人提交的区块链技术存储的电子数据，如果能够证明其在生成、存储、传输、提取等环节的真实性，且经人民法院核验一致的，推定其真实，除非对方当事人有相反证据足以推翻。规则同时也保持了理性，并未给予盲目的背书。第十七条暗示了对上链前数据的审查要求，即需要审查数据来源的真实性，当事人对区块链证据提出异议并提供理由的，法院应当要求举证方提供原件或进行鉴定。

这一规则的重大意义在于，它将区块链存证的效力从“需要自证真实”转变为“推定有效，除非被推翻”，实质上减轻了举证方的负担，降低了维权成本，尤其有利于知识产权保护。

2022 年发布的《最高人民法院关于加强区块链司法应用的意见》从顶层设计层面提出了建设全国统一的人民法院司法区块链平台，提出到 2025 年建成人民法院与社会各行各业互通共享的区块链联盟。这标志着区块链存证从单纯的诉讼证据向社会治理基础设施转型。意见特别强调了要建立健全标准规范体系，确保存证数据的上链前真实性，防止技术被滥用[8]。

2 技术信任与法律真实的鸿沟

尽管法律法规已赋予区块链存证较高的法律地位，但在实际操作中，区块链技术并非完美的“真相机器”。法学界与实务界普遍认为，区块链存证目前面临着严重的断裂，即技术信任与法律真实之间的鸿沟。

2.1 上链前数据的真实性悖论

这是区块链存证面临的最大法律挑战，也是所有电子存证技术的根本性缺陷。区块链只能保证数据上链后不可篡改，却无法保证数据上链时是真实的。这在计算机科学中被称为预言机问题，在数据科学中被称为“垃圾进，垃圾出”。从证据法理的深刻剖析来看，这是因为区块链技术卓越地完成了数据的形式封装与固化，却无法对其指涉事物的本体进行实质背书。如果借贷平台在后台数据库中伪造了虚假的借款记录，然后将这些虚假记录上链，由于区块链的不可篡改性，这些虚假信息一旦上链，反而披上了技术公信力的外衣，变得更加难以推翻。又如在知识产权确权纠纷中，侵权人抢先将他人未发表的摄影作品下载，并以自己的名义在某版权区块链存证平台上进行存证确权。此时，区块链的技术信任仅仅能证明该侵权主体在某一确定的时间戳节点持有了该数字文件并将其上传，但绝无法在法理上推导出该主体就是该作品的合法原创者这一法律事实。

刘品新提出了区块链证据的两大定律：入链后数据真实性有保障，入链前数据真实性需优化[9]。他认

为不能以后者的不确定性否定前者的价值，但必须建立针对上链前数据的专门审查机制。他建议区分直接生成类证据和转化存证类证据，前者可信度较高，后者则需严格审查来源。除此之外，法官要警惕技术中心主义的倾向，不能因为有了区块链就放弃对案件事实本身的实质审查。区块链技术决定了其能自我鉴真，但这种鉴真仅限于数据的一致性，而非内容的客观真实性。

2.2 举证责任分配的公平性危机与技术霸权

《人民法院在线诉讼规则》确立了区块链证据的推定真实效力，这意味着举证责任在某种程度上转移给了否认数据真实性的一方。在司法实践中，这可能导致实质上的不公平。

通常情况下，提交区块链证据的一方是掌握技术优势的大型互联网平台，如电商平台、银行、版权机构，而抗辩方往往是处于弱势的个人用户。个人用户很难从技术层面去证明区块链底层算法存在漏洞，或证明节点合谋篡改了数据。首先，反证难度大。要推翻区块链证据，抗辩方往往需要聘请昂贵的专家辅助人或申请司法鉴定，这在小额互联网纠纷中是不经济的。其次，技术压迫风险。过度依赖区块链的推定效力可能会异化为强势方对弱势方的技术压迫。如果法院不加甄别地采信所有区块链存证，可能会导致大企业利用技术优势制造完美证据，而弱势方无力反驳的局面[10]。

2.3 隐私保护与不可篡改性的冲突

区块链的核心特性是不可篡改和永久保存，而我国《个人信息保护法》日益强调用户的更正权和删除权。但当含有个人隐私、商业秘密甚至错误信息的电子证据被永久写入区块链后，如何执行法律规定的删除义务？虽然可以通过哈希处理实现内容脱敏，但哈希值本身在特定条件下仍存在被逆向匹配的风险。此外，如果是全量数据上链，隐私泄露风险极高[11]。

如果法院最终判决某条上链信息是诽谤或侵权内容，但由于区块链的技术特性无法物理删除区块，受害人的权利将处于持续受损状态，这是一个亟待解决的法律技术难题[12]。在司法链上，为了保证公信力，通常希望节点越多越好，数据越透明越好，但为了保护隐私，又希望数据越隐秘越好，这种矛盾在公有链存证中尤为突出。

2.4 存证平台的资质与中立性风险

并非所有的区块链都是可信的。当前市场上存在大量商业性的私有链或弱中心化的联盟链，这些链的节点往往由运营企业自身或利益关联方控制，缺乏真正意义上的去中心化监督。尤其是部分互联网平台自建的区块链存证系统，既作为数据存储方，又作为纠纷相关方，存在角色冲突。在这种结构中，平台可能选择性上链、仅保存对己有利的证据，或通过控制多数节点影响共识机制，从而削弱了区块链应有的中立性与透明度。一旦存证平台因经营不善倒闭、管理失误导致私钥遗失，或主动关停节点，所谓永久存证的数据将因无法访问或验证而失去意义，链上证据的完整性、持续性亦无从保障。

在司法实践中，部分法官因对技术原理了解有限，仅因存证凭证带有区块链字样即予以认可，未能深入审查其底层技术架构、节点分布、存证时间是否真实、数据哈希值是否在早期阶段已锚定至公链等实质性内容。这种技术迷信可能导致存证平台资质不齐、链体结构封闭等问题被忽视，进而使存证过程存在的程序瑕疵或人为操纵风险被掩盖。有学者统计发现，实践中存在未作说明直接采信的情况，这反映了司法人员对技术本质认知的缺失[13]。

3 中外路径差异与启示

为了更好地完善我国的区块链存证规则，有必要放眼全球，考察美国、欧盟等主要司法辖区的立法与实践经验，运用比较法的方法论，从功能主义与诉讼认识论的高度，提炼出不同司法辖区规制技术证据的底层逻辑与哲学分野。

3.1 美国：市场驱动下的可采性博弈

美国的区块链证据规则呈现出州立法先行与联邦判例跟进的特点，且深受普通法系对抗制诉讼模式的影响。

早在 2016 年，佛蒙特州就通过了相关法案，明确规定区块链上的数字记录只要通过了加密算法的验证，就具有法律效力。特拉华州、伊利诺伊州等也相继立法，承认智能合约和区块链记录的法律地位，这些立法的主要动力是争夺数字经济的中心地位。

在联邦层面，美国并没有专门针对区块链的证据法。美国法院主要依据《联邦证据规则》来审查区块链证据。举证方必须提供足够的证据证明该电子记录是其声称的内容。对于区块链，通常需要专家证人出庭解释系统的可靠性。传闻证据规则是美国法中一个独特的障碍，由机器自动生成的记录通常不被视为传闻，但如果是由人输入的记录存储在区块链上，则可能构成传闻证据，美国法院倾向于利用业务记录例外来解决其可采性问题[14]。

美国模式强调当事人主义，证据的真实性主要靠双方律师在法庭上通过交叉询问专家证人来博弈，法官作为居中裁判者，不会轻易给予推定真实的优待。相比之下，中国模式更强调职权主义和效率，通过司法解释赋予特定区块链平台较高的法律效力，减少了庭审辩论的成本。

3.2 欧盟：eIDAS 框架下的功能等效

欧盟在应对区块链证据效力挑战时，并未采取单独立法的激进策略，而是展现出一种深厚的制度包容性，其核心方法论体现为功能等效原则。

欧盟并未专门针对区块链制定证据法，而是将其纳入《电子身份识别与信任服务条例》（eIDAS）的宏大框架中。根据 eIDAS 条例，符合标准的电子时间戳在法律上具有不可否认性。区块链的时间戳功能被视为一种高等级的电子信任服务，只要区块链服务商符合 eIDAS 关于合格信任服务提供商（QTSP）的要求，其生成的记录在欧盟各成员国法院均具有法律效力[15]。

意大利在 2019 年通过法律规定存储在分布式账本上的电子文档，在满足特定技术标准，即能保证不可篡改性时，具有与 eIDAS 规定的电子时间戳同等的法律效力，这是一种典型的功能等效立法思路。

3.3 比较法启示

通过比较法的方法论提炼可以看出，中美欧三地在应对区块链技术时，本质上是在不同诉讼文化与价值目标指引下，对“技术理性如何转化为法律理性”这一命题作出的不同回应。

我国当前的规制路径展现出强烈的建构主义与国家能力导向。通过最高人民法院自上而下主导建设司法链等基础设施，并利用司法解释直接赋予特定官方平台或合规平台以推定真实的效力，这实质上是在国家公信力的背书下，高效率地完成了对新兴技术的司法驯化。这种效率导向型的职权主义色彩，极大地降低了全社会纠纷解决的整体成本，高度契合我国现阶段解决互联网海量纠纷的实务需求。

然而，比较法的方法论启迪我们，中国模式在保持效率优势的同时，必须警惕技术推定带来的权利失衡风险。在微观的审查机制构建上，特别是当涉及复杂的技术争议及面对棘手的上链前数据真实性难题时，我国诉讼程序亟需吸纳普通法系对抗制审查的认识论精髓。具体而言，应引入类似美国的深度交叉询问机制，允许抗辩方及其聘请的专家辅助人对区块链证据的数据源头、预言机采集机制、平台中立性展开实质性的质证与挑战。这是防范技术垄断、弥补单纯依赖事前平台资质认证所产生的审查盲区的必由之路。

4 构建全链路的法律效力审查体系

面对区块链存证在司法适用中的系统性挑战，单纯在旧有规则上修修补补已无济于事。诉讼法理必须在理论层面构建全链路审查体系，如图 1 所示，此体系不仅是对具体审查步骤的重新排列，更是对既有证据法基础理论的深刻反思与实质性超越，具备显著的理论创新与增量价值。

4.1 构建技术自证与司法辅助相结合的审查机制

传统证据审查的印证理论依赖不同来源的独立证据相互支撑，以达到排除合理怀疑的心证标准。但在区块链语境下，分布式账本的全网同源同构特性，使千万节点上的数据副本沦为同一原件的无限克隆，依赖节点数据的所谓多重印证在逻辑上彻底沦为同语反复的循环论证，导致传统横向多源印证理论在区块链鉴真层面失灵。同时，传统审查呈现事后回溯式特征，法官仅对固化后的孤立证据载体进行静态检验。

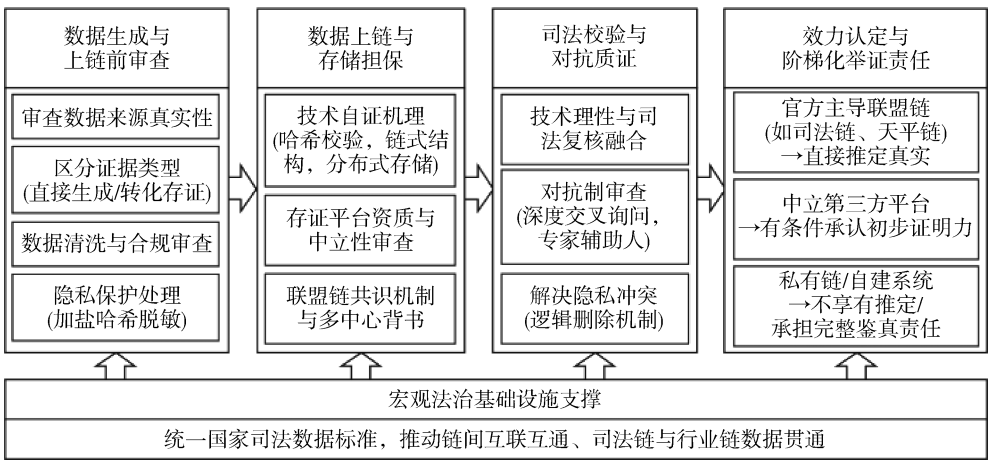

图 1　区块链存证全链路法律效力审查体系

全链路审查体系的理论突破，在于以诉讼认识论的范式跨越，回应技术信任与法律真实的断裂。其一，从载体鉴真迈向生态环境验证。区块链消解了原件与复印件的区分，全链路体系将审查重心前移至证据的生成环境、采集设备与传输通道，将最佳证据规则升维为最佳环境验证规则。其二，从事后静态印证迈向纵向时空过程印证。通过将身份认证、操作轨迹等过程信息与结果数据绑定上链，构建基于生态环境流转的时空印证结构，使孤立的结果证据转化为动态过程证据，系统性抬升造假成本[16]。其三，从单一技术自证迈向技术理性与司法复核的融合。引入公证、司法鉴定等国家公信力节点，开放跨链验证接口，使法官可直接核验原始哈希。这种双重验证模式，有效消解了纯粹算法共识在法律评价中的单薄性，以国家公权力补强技术信任的规范厚度。

4.2 优化举证责任分配规则

举证责任的科学分配是全链路审查体系的程序枢纽。为矫正推定规则泛化导致的技术霸权，应摒弃“一刀切”的机械推定，构建基于存证主体技术架构与信任层级的阶梯化配置模型。

对于最高法“司法链”、互联网法院“天平链”等官方主导的联盟链，其节点由司法机关与权威鉴定机构把控，具备国家信用与技术规范的双重担保，应直接赋予推定真实的证明力。抗辩方须承担严苛的反证责任，提供达到排除合理怀疑的鉴定意见，证明区块链底层存在重大漏洞或遭受攻击。对经备案、中立的第三方平台，有条件地承认其初步证明力。依据武器平等原则，抗辩方提出合理怀疑线索后，举证责任即动态倒置，举证方须补充证明平台中立性、链路完整性与数据清洁性。对利用私有链或内部系统自建的存证，其网络高度封闭、缺乏外部制衡，不享有真实性推定[17]。举证方须承担完整鉴真责任，详细释明生成环境与防篡改逻辑，并接受穿透式质询。

这一差异化配置，旨在通过程序精细化调控，防范技术优势方利用代码制造完美伪证，在保障技术应用的同时维系诉讼结构的实质公平。

4.3 完善上链前的数据清洗与合规审查

针对上链前数据的预言机难题，全链路审查体系将规范延伸至链下物理世界与链上数字世界交汇的数据桥梁地带。在规范构造上，对负责将线下客观状态采集上链的中间服务商，建立严格的市场准入与法律问责机制。预言机服务商被视为特殊的数据受托人，若因其系统漏洞、重大过失或恶意篡改导致链上证据失实并造成损害，该行为不仅构成过错侵权，更应视为传统伪证行为在数字时代的延伸，须承担连带赔偿责任或妨害诉讼的法律责任。这一规制思路实现了证据法审查重心从“死的数据”向“活的数据生成主体”的深层回归。

在应对不可篡改性与被遗忘权的价值冲突时，全链路体系主张法律要求与技术手段深度融合的创新进路。事前预防层面，制定强制性隐私保护国家标准，对涉及隐私或商业秘密的底层数据，上链前必须适用加盐哈希等增强脱敏手段，以高复杂度随机盐值抵御彩虹表暴力破解风险，切断数字痕迹与自然人的识别关联。事后救济层面，面对侵权信息依法应删除的困境，体系提供概念重构与逻辑删除机制，由权限节点在最新区块中写入具有更高法律效力的状态更新标记或撤销宣告证书。此举使底层物理痕迹留存以备合规审计，但在公众展示端、搜索引擎及司法核验界面中，原信息被彻底屏蔽或打上已失效或违法撤销宣告。这种底层维系历史真实性、表层实施逻辑阻断的制度设计，既顺应区块链不可篡改的技术属性，又智慧地实现了《民法典》关于人格权保护的实体法诉求[18]。

4.4 推动司法区块链的标准统一与互联互通

全链路审查体系的效能释放，有赖于超越当前各自为战的“链孤岛”现象，从系统论高度构建宏观法治基础设施。

在制度层面，首要任务是建立国家级数据标准统一体系。国家司法行政机关须统筹制定全国统一的第三方存证平台接入司法链的技术协议与管理规范，形成可量化、可审计的准入标准框架，将系统吞吐量、密码安全等级、司法衔接度及生态开放性纳入多维评级体系。这一国家背书的高等级认证，在宏观上成为服务商优胜劣汰的市场信号；在微观诉讼中则转化为法官采信证据的客观裁量基准，有效限缩技术审查的任意性与盲目性。

进而言之，全链路体系的终极形态是打通司法链与关键社会经济节点的阻隔，实现与国家版权链、金融链、政务链等核心行业联盟链的全面数据贯通。通过建立跨链互认的底层通信协议与合法合规的信息共享框架，法院的角色将从案件事实外部的传统调查者转型为分布式账本内部的数字核验者。以知识产权纠纷为例，法官经授权可一键跨链调取版权链上的原始确权哈希与时间戳[19]，彻底根除多头重复取证造成的社会成本浪费。

这一体系化跨域互通，在程序法层面消解了证据

壁垒与司法内耗，在国家治理战略高度则将司法区块链从封闭的办案工具升级为维系社会底层商业信任的法治基础设施，为全链路审查提供最坚实的宏观支撑。

5 结论

区块链技术推动了电子存证从“自证清白”到“技术自证”的范式转移，降低了信任成本，重塑了证据的生成与认证逻辑。然而，技术只是法律的辅助，而非替代。区块链能证明数据未被篡改，却无法证明事实即为真实，法律真实的认定仍需法官结合链上证据与链下事实，依据逻辑与经验法则综合判断。未来，人工智能与区块链的融合将使存证更加智能，如上链内容自动审查、智能合约执行保全。法律人应拥抱技术，更需坚守正义底线。通过构建上链前审查机制、公平的举证规则和完善的隐私保护，确保信任机器真正服务司法公正。在数字正义的道路上，法律与技术应是并肩同行的伙伴，而非相互排斥的对手。

参考文献

[1] 徐梦梦,涂永前. 刑事电子数据鉴真从区块链到算法的法律规制转型[J]. 浙江工商大学学报,2025(6):77-87.
[2] 杨幸芳. 论区块链存证真实性审查[J]. 中国应用法学,2023(3):175-182.
[3] 王志刚,张雪. 区块链存证证据的真实性审查[J]. 西安电子科技大学学报(社会科学版),2021,31(4):76-84.
[4] 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),2023,44(5):111-119.
[5] 施鹏鹏,叶蓓. 区块链技术的证据法价值[EB/OL]. (2019-04-17)[2026-01-16]. https://www.spp.gov.cn/spp/llyj/201904/t20190417_414991.shtml.
[6] 龚善要. 区块链电子证据与最佳证据规则的适用冲突及其应对[J]. 河北法学,2026,44(2):123-139.
[7] 江必新,王鑫. 论人工智能与法治现代化[J]. 广西大学学报(哲学社会科学版),2025,47(6):85-97.
[8] 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.
[9] 刘品新. 论区块链证据[J]. 法学研究,2021,43(6):130-148.
[10] 谢登科. 电子数据的技术性鉴真[J]. 法学研究,2022,44(2):209-224.
[11] 童云峰. 区块链技术和个人信息权利之冲突与消融[J]. 东北大学学报(社会科学版),2024,26(1):108-116,150.
[12] 赵磊,石佳. 依法治链:区块链的技术应用与法律监管[J]. 法律适用,2020(3):33-49.
[13] 陈永生,苏泽琳. 区块链证据认证形式化问题及克服[J]. 浙江工商大学学报,2024(5):65-77.
[14] Wang Xukang,Wu Yingcheng,Ma Zhe. Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes[J]. Frontiers in Blockchain,2024,7(7):1306058.
[15] 国强,李新友. 欧盟数字身份进展情况研究[J]. 信息安全研究,2020,6(7):582-588.
[16] 庞卢宁. 从“要素”到“结构”:区块链存证电子数据审查新论[J]. 山东警察学院学报,2024,36(1):80-87.
[17] 周祥军. 区块链存证推定规则的理论证成与类型适用[J]. 证据科学,2025,33(6):731-744.
[18] 方义媛,程嘉琪. 论区块链证据在民事诉讼中的审查[J]. 争议解决,2023,9(4):1391-1399.
[19] 赵双阁,孟繁豪. 区块链技术背景下新媒体版权集体管理信息交互与存储模型反思与重构[J]. 中国编辑,2025(9):33-40.

（收稿日期：2026-01-17）

作者简介：

郭明轩（2001-），男，硕士研究生，主要研究方向：刑事诉讼法、数据法学。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部