电子数据区块链存证的理解、适用窘境与进路

卢 宇[1]，王会会[1]，张 永[2]

（1.华东交通大学 人文社会科学学院，江西 南昌 330013；2.青海民族大学 法学院，青海 西宁 810007）

摘 要：电子数据区块链存证是利用区块链所具有的去中心化、可信时间戳、加密算法等技术手段对电子数据进行保存，其法律本质是一种自我鉴真方法。电子数据区块链存证的繁荣发展应从技术和法律两个角度出发：针对入链前电子数据真实性难以认定的问题，技术上，缩短电子数据从产生到入链的时间差；法律上，制定电子数据真实性的司法推定规则。以“技术自证”辅之以“司法公证”形成电子数据存证审查的二元化视角来解决证据资格完全依赖于公证的难题。构建一致性的电子数据区块链存证标准来解决第三方区块链存证平台中立性存疑的问题。

关键词：区块链存证；自我鉴真；真实性；技术自证；平台中立

中图分类号：D925.2 **文献标识码：**A **文章编号：**1008-2395（2023）01-0077-09

收稿日期：2022-09-09

作者简介：卢宇（1971-），女，博士，副教授，主要从事刑法学研究；王会会（1997-），女，硕士研究生，主要从事刑法学研究。

随着互联网的发展，中国网民的数量也在迅速增长，截至2021年12月，我国互联网用户高达10.32亿。网络时代的发展使得电子数据作为纠纷解决中的证据使用概率大为增加，但电子数据本身所具有的虚拟、易篡改、脆弱性又会使得法院在审理涉电子数据的案件时无从下手，导致电子数据被采信率较低。区块链技术的出现为电子数据存证提供了新的技术手段，杭州互联网法院“区块链存证第一案”（以下简称“第一案”）①的宣判也表明，利用区块链存证的电子数据已经被我国司法实务逐步认可，采用区块链技术进行存证，可以最大程度确保证据的同一性和真实性。在电子数据区块链存证成为研究热点的背景下，需要我们理解何为电子数据区块链存证，利用区块链存证有何优势以及会存在何种不足。本文在对电子数据区块链存证的技术性原理以及可行性理解的基础之上，继而探究了其法律本质到底是什么。并通过梳理裁判文书网上414份裁判文书探究存证过程中出现的问题，力求提出相应的完善进路。

一、电子数据区块链存证的技术路径及其可行性

（一）区块链的技术原理

区块链是数字货币发展到一定阶段的产物，同时使用了分布式记账技术、P2P网络、共识机制、加密算法等一系列技术的区块链，本质上是提供拜占庭容错②来确保一致性的去中心化分布式存储系统的数据库[1]。传统的数据库的读写权限掌握在公司、银行或政府手上，具有中心化的特征，然而区块链技术所采用的是读写权限同时由系统中的每一位有能力的参与者共同掌管的去中心化方式，区块链的数据库是只读数据库，即只能创建，不能修改和删除的数据库[2]。在世界范围内，任何有能力的节点都能以成员身份参与到区块链网络之中，在享受平等于其他节点权利的同时，共同承担维护区块

① 参见（2018）浙0192民初81号判决书，同时该案是杭州互联网法院2018年发布的自2017年8月18日挂牌以来的十大典型案例之一：杭州某某文化传媒有限公司诉深圳市某某科技发展有限公司侵害作品信息网络传播权纠纷案——以区块链技术存证的电子证据的认定。搜狐网：http:// www. sohu. com/ a/ 250549319_99971276，上传日期：2018年8月28日，引用日期：2018年10月31日。

②根据百度百科的定义，拜占庭容错（BFT）不是某一具体算法，而是能够抵抗拜占庭将军问题导致的一系列失利的系统特点。这意味着即使某些节点出现缺点或恶意行为，拜占庭容错系统也能够继续运转。这与区块链所具有的去中心化的特征不谋而合。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

链运行的责任。同时，为了确保区块链网络中所存数据的可靠性和一致性，该系统中的所有节点通过共识机制来同步彼此的数据信息。电子数据本身即具有脆弱性、易篡改的缺陷，而区块链技术所特有的不可篡改、多重参与等特性恰好弥补了电子数据本身的缺憾。

（二）电子数据区块链存证的技术路径

电子数据区块链存证，简言之就是将电子数据利用区块链技术进行保存。电子数据从产生到入链，首先需要经过电子数据的收集阶段（数据可以由用户自行收集，也可以由用户委托第三方存证机构收集）。后将收集到的电子数据上传至第三方存证平台，第三方存证平台会生成两个密钥（一个私钥、一个公钥），用户用私钥对电子数据进行签名，第三方存证平台用公钥对电子数据进行加密，再将原始电子数据转化为哈希（Hash）值，Hash 值就类似于人的身份证号码，是独一无二的，不同的电子数据有不同的 Hash 值①，电子数据上每个字母甚至每个符号的改变都会对 Hash 值产生不同的影响。因此，当发生争议时，司法鉴定中心可将后台的 Hash 值与第三方存证平台上传的作对比，若一致，则意味着原始数据未被篡改[3]。虽然将电子数据转化为 Hash 值在一定程度上降低了电子数据被篡改的可能性，但也存在着例外，如前文所述，区块链是由一个个节点组合而成，当电子数据的 Hash 值存储于该服务器终端时，则存在着被篡改的可能性，此时若黑客入侵电子数据，电子数据的 Hash 值则存在着被破坏、篡改的风险。因此，第三方存证平台除了将电子数据转化为 Hash 值之外，还利用了分布式账本技术②，分布式账本技术会将电子数据加盖时间戳，可以实现电子数据的有效记录，为电子数据的真实性加盖了“双重保险”。将加盖时间戳的电子数据以及电子数据的 Hash 值打包上传至区块链平台后就不再需要人为操作，自动化运行的区块链可以促使所有节点，包括公证处、司法鉴定中心以及法院等及时共享区块链上的电子数据信息。电子数据从生成到法庭质证之前的传送过程如图 1 所示：

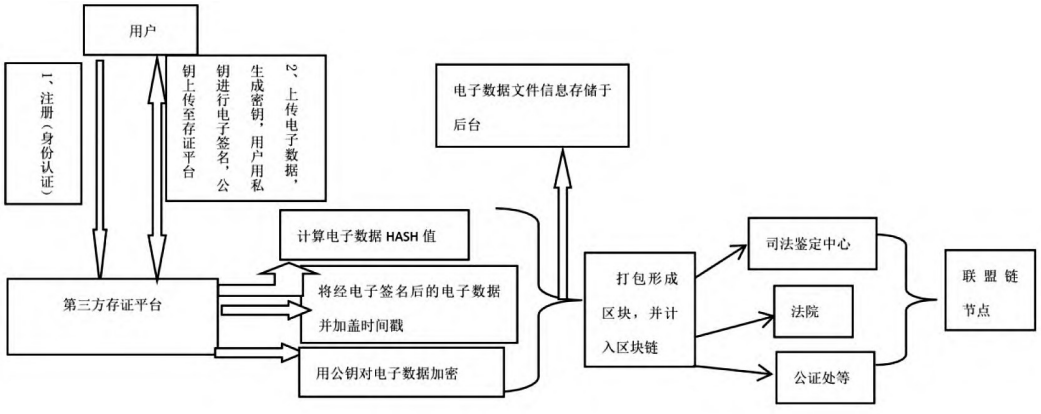

图 1　电子数据区块链存证示意图

（三）电子数据区块链存证的可行性

利用区块链存证的电子数据在保障电子数据的客观真实性、强化电子数据的关联性以及优化电子数据的合法性方面具有重要意义。

在电子数据的客观真实性保障方面：传统电子数据属于中心存储模式，这种存储模式极易受到人的主观干预的影响，而导致电子数据的客观真实性的折损。容易出现合谋篡改、黑客入侵、数据丢失的情形，降低电子数据的可信度。而素有“信任机器”之称的区块链技术，按照时间顺序将数据区块以顺

①电子数据是通过二进制表达的，因而可以设计出一种算法，将电子数据通过二进制算法得到一个长度固定的结果，这个结果即为哈希值，即哈希值是由一连串的代码所组成。

②分布式账本技术即由多方共同维护，使用密码学保障传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

序相连的方式组合成的一种链式数据结构，借助分布式账本技术所特有的去中心化、无法篡改的技术优势，能够有效保障电子数据呈现出原本的样态，因此，将区块链技术应用于电子数据存证之中，可以有效减少主观干预，保障电子数据的客观真实性。

在电子数据的关联性强化方面：电子数据证明案件事实需要满足内容与载体的关联性。即证据与待证事实之间应有最低限度的证明能力。内容关联性是电子数据同案件事实的关联性；而载体的关联性则是电子数据同案件当事人和其他诉讼参与人有关，具体又可分为人、事、物、时、空的关联性[4]。由于电子数据是由 0 和 1 数字信号量所组成的数字空间，其难以确认不同文件之间的关联关系[5]，而区块链是一种记录交易的数据结构，交易信息是区块所承载的任务数据，具体包括交易双方的私钥、交易的数量、电子货币的数字签名等，因此区块链存证可以很好地实现电子数据的关联性追溯。

在对电子数据的合法性优化方面：传统电子数据的合法性包括主体合法、形式合法、内容合法[6]。电子数据区块链存证除了关注上述所述合法性之外，还满足了存证程序的合法性。合法性要求电子数据符合法律规定，即区块链技术在存证中的应用只要在法律规定的范围内进行即可。区块链是由数个区块组合而成，区块中包含前一区块形成的 Hash 散列，前一区块形成的 Hash 散列用来将区块连接起来，实现交易的顺序排列[7]，提升了电子数据存证程序的公开透明度，确保了区块链存证的合法性。

二、电子数据区块链存证的法律本质——自我鉴真方法

在诉讼过程中，实物证据材料面临着被篡改、伪造的风险。司法实务人员为应对这一风险，引入了实物证据鉴真规则，实物证据鉴真即对实物证据的真实性予以证明的过程。而电子数据虽然不具有实物形态，但其作为法定八大类证据种类之一，其在生成、收集的过程中也面临着被篡改、伪造的风险，因此，其也应遵循实物证据鉴真规则，由此产生了电子数据鉴真[8]。区块链技术出现之前，对电子数据的鉴真主要依靠司法机关的公证及信用背书，但公证会增加当事人的诉讼负累，降低法官的办案效率。自“第一案”以来，电子数据的取证、存证阶段逐渐引入了区块链技术，有效弥补了依靠公证审查电子数据真实性的缺陷。可以说，区块链技术应用于存证过程中在一定程度上实现了电子数据的自我鉴真。详言之，分布式账本技术的应用在一定程度上实现了电子数据的外部鉴真，如前文所述，区块链同时使用了分布式账本技术、共识机制等技术手段，分布式账本技术使得每一笔交易记录都会被加盖时间戳，具有过程不可逆性、篡改会留痕的特征，这一技术特征可以实现入链电子数据的有效记录，因此属于电子数据的外部鉴真。而 Hash 算法的运用则实现了电子数据的内部鉴真，利用 Hash 算法将电子数据计算出的 Hash 值具有独特性，不同电子数据具有不同的 Hash 值，Hash 值具有唯一性，对电子数据的任何细小改动都会导致 Hash 值的变化，例如改变一个标点符号都会导致 Hash 值的变化，继而导致入链电子数据内部结构发生变化，因此 Hash 算法的运用属于电子数据的内部鉴真。外部鉴真抑或内部鉴真，都是利用区块链本身所具有的技术特征来实现的，因此，区块链技术应用于电子数据在本质上提供了一种自我鉴真方法。

三、电子数据区块链存证的适用窘境

随着网络时代的发展，电子数据在法庭上的适用的频率也越来越高。2018 年的“第一案”开辟了区块链技术应用于电子数据存证的先河，区块链技术的运用在保障入链电子数据的客观真实性、增强关联性以及优化合法性等方面具有相当的优势，不再赘述。与此同时，区块链存证电子数据在司法实务中的适用也存在相当的窘境，以中国裁判文书网 2018 年至今的民事案件为样本，以“电子数据”“区块链”“存证”为关键词进行搜索，审结程序为民事一审，涉及电子数据区块链存证的裁判文书 447 份，剔除无效样本 33 份，剩余 414 份有效样本。这些案件清晰地反映了区块链存证电子数据在实务中面临的窘境。详言之，主要表现为以下三个方面：

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

（一）区块链存证对于链前产生的电子数据的真实性难以保证

电子数据在产生阶段的真实性，是传递过程真实性的前提[9]。虽然最高人民法院于2018年发布的《关于互联网法院审理案件若干问题的规定》中具体详细描述了电子数据生成、收集、传输过程的真实性①，但在实际的操作过程中，难以保障电子数据产生阶段的真实性。电子数据区块链存证模式可以分为两种，其一是链上产生、事中存证模式，即电子数据从产生到入链是同步完成的。意即用户在区块链系统上从事相应的活动，生成相应的电子数据在链上保存，例如比特币、以太币、莱特币等虚拟货币的交易就是如此。其二是链前产生、事后存证模式，在司法实践中，绝大部分的存证模式即是此种模式，在此模式下，当事人通过交易产生了电子数据，而后发生纠纷，当事人双方或一方利用区块链进行存证，例如微信聊天记录截屏、双方当事人签订的借贷（买卖）合同等均是事前产生，利用区块链进行事后存证模式。毋庸置疑，事中存证模式之下，电子数据可以依仗区块链技术本身的技术优势来保障电子数据的真实性，在此种存证模式下，电子数据本身就是在链上生成的，故无须考虑其入链之前的真实性；但在事后存证模式下，行为人为了自身利益可能会将篡改后的电子数据再上传至区块链存证平台，此时电子数据则面临着真实性难以保证的问题[10]。例如在（2019）京0491民初1212号民事判决书中互联网法院认为电子数据不同于传统的证据方式，其具有真伪不明的脆弱性，并非采用了时间戳等技术手段所采集的电子数据就是真实的，存在抓取之前因所处设备或网络环境存有问题而被破坏的可能性。详言之，原告并未按照《操作指引》中的“互联网连接真实性检查”的操作流程来进行操作：一是没有点击“局域网”设置查看代理情况，存在设置虚拟代理网站的可能；二是“ipconfig”没有加上“/all”，就不会显示DNS等关键信息，无法排除存在虚拟网站的可能；三是没有执行“tracert目标网页域名”，无法确定接入网站的真实性。原告取证过程中前置性检查中三个步骤的缺失导致原告提供的可信时间戳证据不足以取信，难以证明电子数据在生成时期的真实性②。与此同时，行为人对入链之前的电子数据也会存在多版本预留的情况，这也会影响电子数据的真实性，如在（2020）京0491民初19386号一审民事判决书中③，法院认为被告提交的中国庭审公开网庭审公开视频中关于被告举证的时间戳证据，明显系通过技术手段先对某一公众号进行了篡改，然后再进行时间戳固证，存在多版本预留的情况，因此该份证据的真实性、合法性、关联性均不予认可。

（二）区块链存证并未有效发挥“技术自证”的优势

传统电子数据的收集、保全大多由当事人单方完成，存在着为了自身利益对电子数据进行修改的风险，因此传统电子数据的真实性需要补强，而补强传统电子数据真实性的常用方法是对其进行鉴定或公证。但如前文所述，区块链技术具有全程记录、不易篡改、数据加密的特性使得入链的电子数据真实性更高，通过“技术自证”的属性改变了传统电子数据的“国家公证”模式。但根据三大互联网法院电子诉讼平台实时滚动的数据条显示，利用区块链存证的在线交易（使用）条数远远低于在线采集数据的数量：例如由表1可知，三大互联网法院在线采集数据数均高达上亿条，但交易条数最高的为北京互联网法院，仅为30 268条，验证数占采集数的比重基本可以忽略不计，由此可知通过区块链存证的电子数据的采信率极低。

①《最高人民法院关于互联网法院审理案件若干问题的规定》电子数据的真实性的认定，应当审查判断电子数据生存、收集、存储、传输过程的真实性，并着重审查以下内容：1.电子数据生存、收集、存储、传输所依赖的计算机系统等硬件、软件环境是否安全、可靠；2.电子数据的生成主体和时间是否明确，表现内容是否清晰、客观、准确；3.电子数据的存储、保管介质是否明确，保管方式和手段是否妥当；4.电子数据提取和固定的主体、工具和方式是否可靠，提取过程是否可以重现；5.电子数据的内容是否存在增加、删除、修改及不完整等情形；6.电子数据是否可以通过特定的形式得到验证。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或者通过电子取证存证平台认证，能够证明其真实性的，法院应当确认。

②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、侵权纠纷一审民事判决书，（2019）京0491民初1212号，与之类似的有（2020）沪0115民初3682号等文书。

③北京华视聚合文化传媒有限公司与宁夏博鹏电子商务有限公司侵害作品信息网络传播权纠纷一审民事判决书（2020）京0491民初19386号。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

表 1　区块链采集数据数与交易数据数对比[①]

互联网法院	在线采集数据数 / 条	在线验证、交易数据数 / 条	验证数占采集数的比重 /%
北京	155 045 396	30 268	0.02
杭州	251 086 873	256	0.000 1
广州	273 546 853	7 562	0.003

出现上述问题的最大原因是司法机关对仅通过区块链存证的电子数据持保留的态度。实践中，部分当事人为了增强电子数据的采信率，常常通过区块链对电子数据进行存证以后，会选择到公证处进行公证，由此可知对区块链电子数据资格审查仍然是采取公证的形式。而对于仅依照区块链存证的电子数据，则受到了司法机关关于技术本身、存证环境的清洁度遭受质疑而难以被法院采信的影响。这也在一定程度上说明了经区块链存证的电子数据的证据资格的审查仍然离不开国家的公证信用背书，区块链技术未发挥其特有的技术优势。

表 2 摘取（2022）粤 15 民初 45 号、（2021）吉 06 知民初 16 号、（2022）湘 0105 民初 1132 号对经公证后的电子数据的真实性的认定说理较为周全的三份裁判文书样本来直观感受一下：

表 2　对公证机构的裁判文书说理情况

案号	公证机构	关于公证机构的具体论述
（2022）粤 15 民初 45 号	国信公证处	原告提交的宁夏回族自治区银川市国信公证处出具（2021）宁银国信证字第 7317 号公证书证明其提供的证据的真实性，本院予以采纳。
（2021）吉 06 知民初 16 号	公证保	在保管过程中采用中科院国家授时中心提供的网络时间服务器进行时间校对，采用非对称性的 SHA256 加密算法对数据进行加密传输，实现了电子数据的可靠采集、不可篡改，确保已保管的电子数据与取证结果的一致性、完整性。
（2022）湘 0105 民初 1132 号	杭州互联网公证处	向本院提交杭州互联网公证处出具的《电子数据取证与区块链存证证书》，该证书取证时间为 2021 年 8 月 2 日，经比对，该文内容与原告在今日头条网站上发表文章的部分内容一致。

根据表 2 可知，无论是在（2022）粤 15 民初 45 号判决书中原告提交的国信公证处出具的公证书，还是在（2021）吉 06 民初 16 号公证保采用中科院提供的加密算法，抑或是在（2022）湘 0105 民初 1132 号杭州互联网公证处出具的公证书，都说明实务中均采用公证的方式来保障电子数据的真实性。如前文所述，区块链存证的电子数据可以实现自我鉴真，电子数据经过区块链上自带的 Hash 值以及分布式账本技术的验证后就能证明该电子数据的真实性，这在一定程度上实现了区块链存证电子数据的技术自证，在可以技术自证的前提下，是否必须要对电子数据双重验证？[11]

（三）第三方区块链存证平台中立性遭受质疑

首先，第三方存证平台资质审查并无统一的标准。目前，尚未有相关的法律法规设置存证平台的资质审查标准，而在司法实务中各个互联网法院虽也对第三方区块链存证平台资质审查制定了相关的标准，但审查标准各有侧重，并没有统一的适用标准。这里选取说理较为详细的（2019）京 0491 民初 17647 号、（2019）京 0491 民初 37452 号、（2022）赣 05 民初 15 号等代表性判决，如表 3。可以发现平台资质审查标准各有不同，甚至于同一法院在同时期的不同判决中针对存证平台都会有不同的审查认定标准，如（2019）京 0491 民初 17647 号认定角度是第三方存证平台提供的服务是否符合相关的法律规定；而在

①分别详见北京互联网法院“天平链”平台 https://tpl.bjinternetcourt.gov.cn/tpl/、杭州互联网法院“司法链”平台 https://blockchain.netcourt.gov.cn/，以及广州互联网法院“网通法链”平台 http://bc.gzinternetcourt.gov.cn:9001/gzinternetcourt-evidence/index.html#/netcomchain，最后一次访问为 2022 年 8 月 31 日晚上 9 点 14 分。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

（2019）京0491民初37452号中审查角度是存证技术是否经过了国家级质量监督检测，即使提供的服务符合相关的法律规定也不足以作为采信的依据。第三方存证平台资质审查缺乏标准化的治理，会导致当事人为了确保电子数据的可信度，倾向于在多个平台上进行存证，这将大大折损存证平台的中立性。

表3 存证平台资质审查要点

案号	审查要点	关于存证平台资质审查的具体论述
（2019）京0491民初724号	第三方存证平台是否链入互联网法院区块链系统	北京版权家科技发展有限公司具备第三方存证平台资质，2019年跨链接入北京互联网法院天平链系统后，存证用户在该存证平台存证的同时，北京互联网法院天平链系统会对其存证证据的Hash值进行同步存储，故第三方存证平台提供的电子数据具有真实性。
（2019）京0491民初37452号、（2021）闽06民初717号	存证技术是否经过了国家级质量监督检测	真相网络科技有限公司依法成立并独立于原被告，其运营的IP360电子数据保全平台通过了公安部安全与警用电子产品质量检测中心的检验认证，具备作为第三方电子存证平台的资质。
（2022）赣05民初15号	存证技术是否经过专业、权威的第三方机构认可	原告提供的可信时间戳认证证书是由我国专业、权威的第三方存证平台颁发。

其次，第三方存证平台自身具有营利性。第三方存证平台大多数是以营利为目的的公司。俗话说“吃人嘴软、拿人手短”，很多当事人会认为第三方存证平台因收取了当事人的费用，在为当事人提供服务的过程中有为了自身利益而篡改证据之嫌疑，继而会导致其中立性、信誉度丧失。因此，可能会受到对方当事人关于其收集、固定的证据不具有客观性，不足以被采信的质疑。

四、电子数据区块链存证的适用进路

将区块链技术适用于电子数据存证过程中源于两种力量，其一是司法实践的现实需求，随着互联网时代的发展，电子数据的广泛运用，实务中需要新的思维工具来优化办案模式以及提升工作效率。其二是区块链电子数据自身发展的需要。区块链存证电子数据需要将其技术应用于实践并不断得到实践的认可与否定，在认可与否定中不断攻克难题[12]。可以说，电子数据区块链存证在一定程度上实现了法律与技术的融合发展。但利用区块链存证的电子数据在司法实践中面临着入链之前的真实性难以保证、证据资格审查仍然依赖于公证，并未发挥技术自证的优势以及第三方存证平台遭受质疑的问题。本文认为，既然电子数据区块链存证是技术与法律融合发展的产物，在面对上述问题时，理应从技术和法律两个层面提出相应的完善进路（这里需要特别说明的是，技术与法律在电子数据区块链存证中的融合发展并无孰先孰后之分，区块链技术的发展不得超越法律的框架，而法律具有滞后性，法律的发展也要依赖于区块链技术的进步）。针对电子数据入链之前的真实性难以保证的问题，在技术层面：缩短电子数据从产生到入链的时间差；在法律层面：制定链下生成的电子数据的司法推定规则；将电子数据分为链上生成和链下生成进行区分审查，形成电子数据区块链存证审查的二元化视角来解决证据资格依赖于公证的难题；构建一致性的电子数据区块链存证标准、确保相关平台的中立性。详情如下：

（一）技、法平衡：保障链下生成的电子数据真实性

如前文所述，电子数据在产生阶段的真实性是保障后续真实性的前提，目前学界虽已关注链下生成的电子数据的真实性，但并未提出相应的完善举措。这里认为可以从技术和法律两个维度来寻求相应的完善进路。

在技术层面，缩短电子数据从产生到入链的时间差。如前文所述，电子数据区块链存证大体上可分为两种模式，其一是事中生成、事中存证，即电子数据的产生与入链是同步进行的，换言之，电子数据是在区块链中产生的，在此种模式之下，发挥了区块链所具有的独特的技术优势，电子数据的真实性得到了有效保障，采信率极高。其二是事前生成、事后存证模式，司法实践中多为此种模式，在此种模式之下，电子数据在入链之前就潜伏着真实性、完整性难以保障的危险。据此，若将电子数据从产

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

生到入链之间的时间差尽可能地缩短，最大程度地保障电子数据的生成时间接近入链时间。那么电子数据在入链之前被篡改、伪造的风险则会大为降低，电子数据的真实性得到有效的保障，采信率也会得到有效的提升。然而，如何缩短电子数据从产生到入链之前的真实性，需要精通区块链的技术人员从技术方面进行搭建。

在法律层面，制定链下生成的电子数据的司法推定规则。司法推定是针对证据的真实性和可靠性问题的解决的一种有效的方法，所谓司法推定是指由法官按照经验法则，从基础（已知）事实到推定事实，并允许当事人提出反证的一种证据法则 [13]。基础事实与推定事实之间的常态联系是推定规则适用的基础。司法推定的前提是推定规则的制定 [14]，因此首当其冲的是制定电子数据存证的推定规则。首先是否及时入链，这是推定电子数据真实性至关重要的一环。如果电子数据在生成之初就已经入链或者在入链之前已经被前端控制，就可以推定为上传到区块链的电子数据是真实有效的。但如果该电子数据是案件受理不久前集中上传到区块链的，则该存证人就可以被推定为存在造假的动机或者是其他的不可靠的因素；其次电子数据的系统完整性是衡量其入链之前真实性的关键环节。完整的电子数据证据链应该包含三个方面：（1）内容数据；（2）附属信息；（3）关联痕迹。若行为人提交的数据链只存在其中的一种或两种，法官可以结合其他关联证据进行相互印证，此时可以参照最高人民法院于 2021 年 5 月份发布的《人民法院在线诉讼规则》① 第十八条的规定，针对上链前数据的具体来源、生成机制、存储过程、第三方见证等进行审查作出综合判断。若存在疑问的，可以要求当事人提供说明，若法官的内心确信达到排除合理怀疑的标准时，可以据此推定该证据是真实的；若当事人无法说明或法官无从求证的，则可以称之为“孤证”，而“孤证”的结构性缺失，则无法作为认定案件事实的依据。

（二）综合考量：形成电子数据区块链存证审查的二元化视角

如前文所述，法院、公证处、司法鉴定中心为区块链电子数据资格审查提供信用上的背书，其本质上仍然是公证。目前在我国司法实务中对区块链存证的电子数据是否经过国家公证仍然非常重视，采用公证方式对区块链存证的电子数据进行背书在增强电子数据的真实性方面具有一定的合理性。但公证会增加当事人的诉讼负累，降低法官办案的效率。有论点提出针对区块链技术与生俱来的去中心化的特点，应赋予电子数据区块链存证与技术相匹配的独立证据资格，同时免除过高的检验义务 [15]，即由原来的依赖公证转向技术自证。这里认为应结合区块链的技术特性并结合电子数据的生成场景进行区分认定，以“技术自证”辅之以“司法公证”，使得技术规范与法律规范协调发展才是电子数据区块链存证发展之王道。

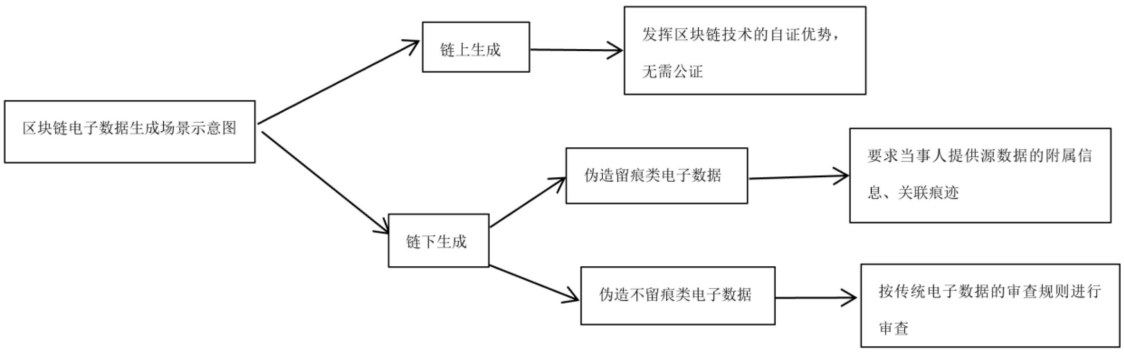

图 2　区块链电子数据生成场景示意图

① 《人民法院在线诉讼规则》第十八条规定，人民法院根据案件情况，可以要求提交区块链技术存储电子数据的一方当事人，提供证据证明上链存储前数据的真实性，并结合上链存储前数据的具体来源、生成机制、存储过程、公证机构公证、第三方见证、关联印证数据等情况作出综合判断。当事人不能提供证据证明或者作出合理说明，该电子数据也无法与其他证据相互印证的，人民法院不予确认其真实性。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

具体来说，如图2所示，区块链技术在存证中的应用被一分为二，即分为链上生成型电子数据与链下生成型电子数据；前者是数据在区块链系统生成并存储，所发生的所有交易记录都是在链上记录、保存，从区块链系统所调取的该电子数据即为原始证据[16]。对于链上生成型电子数据，该类数据自带自我鉴真的属性，应发挥区块链的技术自证的优势，直接认定其真实性，无须公证或信用背书，除非有相反的证据可以反驳。链下生成型电子数据，是指通过区块链抓取、存储、传输的电子数据。对于链下生成的电子数据需要司法机关具体审查。详言之，根据数据是否容易伪造可采取不同的审查路径，具体如下：一是对于伪造留痕类电子数据，如通过互联网诽谤纠纷案件中，原告通过网页形式保全的侵权文章、侵权图片。应同时要求当事人提供源数据来用于法庭校验、源数据附属的数据信息、关联痕迹数据显示数据在生成、存储、传递、修改等情况是否符合链上数据的描述，足以证明上链前未被篡改的，在无相反证据足以推翻的情况下，应认定其具有真实性；二是对于伪造不留痕类电子数据，鉴于其实质上是书证、物证的电子转换，仅是对某一事物或某一时间或地点状态的固化，按照传统的电子数据审查规则来审查即可，换言之，其真实性仍需要通过与其他证据的组合来验证，例如，借款合同纠纷案件中的当事人仅提交的买卖合同电子数据不足以证明电子数据的真实性，法院在审查时需要结合区块链存证证明书、公证处提供的公证文书、客户摘要信息、个人贷款对账单和庭审录音录像等证据来审查电子数据的真实性。

（三）平台中立：构建一致性的第三方区块链存证平台标准

针对第三次存证平台审查并无统一适用标准的问题。首先，由司法机关制定专门的第三方区块链存证平台的具体审查标准，包括存证平台准入的门槛、存证流程的制定。在准入门槛方面，以第三方存证机构取得相应的技术资质为前提，对于第三方存证机构实行审查制，经过严格审查方可从事相关的业务；在存证流程方面，对于用户注册时提供的身份信息标准，参照公证机构进行。其次，建立统一的区块链电子数据存证平台。由司法机关牵头，存证平台参与，统一的电子数据平台应链入司法区块链，这样可以使得第三方存证平台加入司法联盟链，作为司法联盟链的节点。传统的联盟链由法院、公证处、司法鉴定中心等组成，节点可能只有几十个抑或是上百个。区块链作为一种新的技术手段，并非无懈可击，其也会面临着黑客入侵节点的风险，当联盟链上的节点被篡改达到51%时，整个链条便会崩塌。但随着第三方存证平台的加入，联盟链上的节点会变得浩如烟海，联盟链上的节点越多，黑客破坏的风险也就越小。

针对第三方存证平台具有营利性的问题。随着数字经济时代的深入发展，第三方区块链存证平台作为数字市场经济下自发性的产物也会日益庞大，企业具有逐利的心理，在巨额利益的诱惑下，可能会罔顾法律，肆意修改入链的电子数据，存证平台的中立性、信誉度也会大打折扣。为确保存证平台的中立性，相应的互联网法院可以和专业机构进行合作，邀请专业机构对第三方存证平台的后台运行进行权威测评与定期检查其周遭环境的是否清洁、所使用的技术手段是否稳定可靠、是否能够确保电子数据在存证过程中的完整性、是否具备持续提供服务的能力，从而确保第三方存证平台的建设、运营等的健康质量，并发放合规证书。

五、结语

近年来，法律与互联网的融合逐渐成为新的研究热点。区块链与电子数据的融合正是在此背景之下形成的，和互联网一样，区块链正在呈现蓬勃发展之势，电子数据利用区块链进行存证可以有效保障电子数据的真实性、客观性，减少人为干预。但电子数据区块链存证也并非是完美无瑕的，以当前电子数据区块链存证的司法适用为例，电子数据区块链存证尚且有相关问题亟待解决。除了上述提到的问题以外，其也面临着51%的攻击问题，即黑客入侵区块链，当节点被篡改达到51%时，被修改的数据占大多数，原始数据则可能被识别为虚假而被抛弃，就会破坏区块链去中心化的特性，这也意味着区块链网络被完全摧毁，电子数据的真实性、完整性则无法保证。与此同时区块链企业及其业务存

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

在法律监管上的缺失，如何利用区块链中的智能合约技术实现智能监管也是亟须解决的问题。出现这些问题背后的深层次原因是技术与法律并未得到合理的融合，技术与法律要协同发展，切忌“一条腿走路”，技术的发展应在法律的框架内进行，不得超越法律；法律的发展也要依赖于科技的进步，未来电子数据区块链存证的发展理应在法律与技术之间寻求一个平衡点，不得偏废任何一方，为法律技术规范提供一个指引才是应然之道。总而言之，当我们将可靠的技术与正义的担当相互融合时，社会会变得更加安全，世界会变得更加稳定。

参考文献：

[1] 毛荣．“区块链＋电子证据保全”制度研究 [D]. 成都：四川省社会科学院，2019.

[2] 孔涵．以区块链技术助推供应链金融升级分析 [J]. 鲁东大学学报（哲学社会科学版），2022（3）：91-96.

[3] 石冠彬，陈全真．论区块链存证电子数据的优势及司法审查路径 [J]. 西南民族大学学报（人文社会科学版），2021（1）：67-73.

[4] 刘品新．电子证据的关联性 [J]. 中国检察官，2017（9）：75.

[5] 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.

[6] 刘品新．论区块链存证的制度价值 [J]. 档案学通讯，2020（1）：21-30.

[7] 彭帅兴．区块链从入门到精通 [M]. 北京：中国青年出版社，2019：10.

[8] 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.

[9] 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 [J]. 法学研究，2018（4）：121-138.

[10] 王超．区块链技术证明的三重限度 [J]. 学习与实践，2022（1）：56-66.

[11] 胡萌．区块链电子证据的效力分析与规范路径 [J]. 证据科学，2021（1）：31-40.

[12] 沈红卫，刘璐．区块链刑事诉讼电子数据存证、法理基础、实践及前瞻 [J]. 时代法学，2022（4）：32-39.

[13] 刘全友．证据法（新编）[M]. 北京：中国政法大学出版社，2003：263.

[14] 叶蓓．美国区块链证据规则及其启发 [D]. 北京：中国政法大学，2020.

[15] 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.

[16] 段莉琼，吴博雅．区块链证据的真实性认定困境与规则重构 [J]. 法律适用，2020（19）：149-163.

[责任编辑：刘媛]

Application and Approach of Electronic Data Block Chain Storage Certificate

LU Yu[1], WANG Huihui[1], ZHANG Yong[2]

(1.Faculty of Humanities and Social Sciences, East China Jiaotong University, Nanchang 330013, China;
2. Law School, Qinghai Minzu University, Xining 810007, China)

Abstract: The essence of electronic data block chain storage is to save electronic data and a self-identification method by law. To prosper electronic data block chain storage, technology and law should be considered. Technologically, it is to shorten the time from the generation of electronic data to the entry of the chain; in law, the judicial presumption rules for the authenticity of electronic data should be made. With the help of technology and law, the problem that the evidence completely depends only on notarization can be solved.

Key words: block chain storage certificate; self-identification; authenticity; technology proof; platform neutrality

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net