

论区块链证据

刘品新*

内容提要：区块链证据泛指基于区块链技术的一切证明材料，可以具体化为区块链生成、存储与核验之证据。得益于高新技术的加持，区块链证据在厘清涉众复杂案件事实、运用海量异构证据办案与提升智慧司法探索水平等方面独具价值。法律及规范对该新生事物应采取理性态度，遵循同等性对待与差别性归位的原则，并聚焦于真实性问题进行规则适配。缘于哈希校验、时间锁定与节点印证等技术特点，区块链证据在真实性方面得到极大增强，呈现出入链后数据真实性有保障、入链前数据真实性可优化两大定律。我国应以此两定律为技术基础，以既有电子证据真实性规则为制度基础，检讨2021年最高人民法院《人民法院在线诉讼规则》新设条文的不足，挖掘域外探索中可资借鉴的经验，从而构建对区块链证据真实性予以推定、司法认知的规则。

关键词：区块链证据 电子证据 证据规则

一、问题的提出

区块链技术发展至今，经历了数字货币、智能合约、全面应用的三阶段迭变。如今，区块链记录用作证据也已成为司法实践的客观现实。例如，截至2021年8月，北京互联网法院的“天平链”平台已完成版权、互联网金融等9类25个应用节点数据对接，上链数据超过7500万条，跨链存证数据达到数亿条，在线证据验证数大约25000次；杭州、广州互联网法院亦依赖基于区块链技术的电子证据平台进行海量数据累积；最高人民法院同其他各级法院、多元纠纷调解平台等，搭建了“人民法院司法区块链统一平台”。法院系统正在将区块链用于存证的工作，打造为“网上案件网上审理”的一张名片。又如，我国一些权力机关、企事业单位、行业组织在政务服务、^[1]

* 中国人民大学法学院教授，中国人民大学刑事法律科学研究中心、未来法治研究院研究员。

本文为2020年中央高校建设世界一流大学（学科）和特色发展引导专项资金支持项目“科技革命与未来法治跨学科研究平台”的研究成果。

[1] 例如，截至2020年7月，北京市政务服务领域区块链应用落地140个应用场景。参见北京市区块链工作专班专家组：《北京市政务服务领域区块链应用创新蓝皮书（第1版）》，第25页，http://www.beijing.gov.cn/fuwu/lqfw/ztl/yshj/dt/202007/120200715_1948852.html，2021年8月26日最后访问。以下脚注中网页资料的最后访问时间均为此日，不再一一注明。

公益诉讼、〔2〕版权保护、〔3〕中介服务等领域推行区块链系统建设，产生了规模可观的证明材料。刑事诉讼中，比特币、以太币、泰达币等形形色色的数字货币或其数据被用于定罪量刑。〔4〕民事、行政诉讼中，智能合约等文本被用于司法办案。〔5〕据调研了解，2020年，我国几乎所有省份都有了区块链服务平台，北京、上海均已超过18万家，〔6〕其中不乏产出用于司法证明的此类材料。

区块链记录用作证据的问题，引发了我国法律界的广泛关注。〔7〕现有研究涉及区块链记录用作证据的具体场景、实践运用及制度配套等，且出现了明显的观念对立。有论者认为，在未来“所有涉及记录和验证的领域，包括司法过程中的证据保存、提交和验证，都可以借助区块链技术来完成”；〔8〕“区块链证据的法治意义绝不仅限于‘新兴电子证据’这一简单定位，而是对现行证据法体系的一次全面革新”。〔9〕也有论者认为，就当前司法实践的适用情况看，区块链存证技术的适用率并不理想。〔10〕

在规范层面，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》（以下简称“互联网法院审理案件规定”）宣示性地承认，“当事人提交的电子数据，通过……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”。然而，此条文并无实质性的制度进步意义。2021年最高人民法院《人民法院在线诉讼规则》（以下简称“在线诉讼规则”）第16条至第19条，细化了区块链证据的效力、审核规则、上链前数据的真实性审查、补强认定等内容。然而，此类规定在基本概念上严重偏窄，其规则同现行证据规则脱节，对未来法治建设亦无实质性助益。如何改进相关规范，亟待学术界对区块链证据进行基础理论建构。

值得注意的是，全球其他法域基于区块链在数字货币或资产、证券市场治理、交易合规监管、贸易清算或结算等领域的运用，对相关记录用作证据的可采性问题作出了值得关注的三种回应：有的颁行专门承认区块链证据的新法律，有的修订现行法律，还有的则发表了澄清现行法律的声明。〔11〕面对世界范围内“法律+科技”融合发展的制度竞争态势，我国应以固本强

〔2〕例如，湖北省武汉市人民检察院建立了“公益诉讼线索挖掘和区块链存证平台”，浙江省杭州市西湖区人民检察院在专项监督活动中使用了“检察区块链取证设备”。

〔3〕例如，趣链科技等平台提供数字作品的区块链服务，中国版权保护中心在数字作品上应用区块链技术。参见高奇：《〈证据新规〉下版权诉讼中的区块链证据：需求、规制及治理应对》，《电子知识产权》2020年第9期，第93页以下。

〔4〕例如，在“币圈第一大案”中，一、二审法院认定该案涉及比特币等8种虚拟货币，折合人民币达148亿元。参见江苏省盐城市中级人民法院（2020）苏09刑终488号刑事裁定书。

〔5〕智能合约被全面应用于赠与、众筹、买卖、捐款、遗嘱等民事活动中。参见杨廷超：《论数字货币的法律属性》，《中国社会科学》2020年第1期，第98页。

〔6〕据中国科学院信息工程研究所熊刚研究员团队测算，2020年，全国主要省份的区块链服务平台数量为北京183600个、上海183555个、天津84432个、浙江81933个、贵州47098个、海南25872个、湖北20036个。

〔7〕参见前引〔3〕，高奇文；刘品新：《论区块链存证的制度价值》，《档案学通讯》2020年第1期；曾梦：《区块链信息的证据属性研究》，《信息安全研究》2020年第6期；郑观、范克韬、吴泓：《区块链电子证据真实性的认定路径》，《人民司法（应用）》2020年第4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》，《法学杂志》2020年第2期；陈全真：《区块链存证电子数据的司法适用》，《人民司法（应用）》2019年第4期。

〔8〕郑戈：《区块链与未来法治》，《东方法学》2018年第3期，第83页。

〔9〕张玉洁：《区块链技术的司法适用、体系难题与证据法革新》，《东方法学》2019年第3期，第99页。

〔10〕参见罗恬漩：《民事证据证明视野下的区块链存证》，《法律科学》2020年第6期，第68页。

〔11〕See Alexia Pollacco, *The Interaction between Blockchain Evidence and Courts-A Cross-Jurisdictional Analysis*, BCAS, Apr. 23, 2020, https://blog.bcass.io/blockchain_court_evidence.

基促制度发展,“提升国际话语权和规则制定权”。^[12] 本文对区块链技术影响司法证明持积极而审慎的态度,致力于全面阐释、提炼区块链记录用作证据的涵义、样态与价值,并深入论证区块链证据的理性观念、真实性规律与框架性规则。

二、区块链记录用作证据的理论基础

(一) 区块链记录用作证据的原理展开

在证据数字化的时代,区块链技术对司法证明的影响,集中体现为区块链相关材料能否及如何用作证据的问题。所谓区块链,是指“使用密码技术链接将共识确认过的区块按顺序追加而形成的分布式账本”。^[13] 关于区块链的完整描述最早见于《比特币:一种点对点的电子现金系统》一文。^[14] 在该文中,区块和链被解释为用于记录比特币交易账目的数据结构:“区块”是区块链的数据单元,是生成时间段内的所有交易记录;^[15] “链”是由区块按照发生顺序串联而成的日志单元,是整个账本状态变化的记录,分为“公有链”“私有链”“联盟链”。^[16] 这些构成元素表达了一种对数据进行区块分割、前后衔接的存储方式,由此形成的区块链平台类似维基百科或 Google Docs 等其他公开更新的数据库。^[17]

对区块链进行技术解读时可以不惧繁杂,但开展司法适用时则应以简驭繁。以一起侵害作品信息网络传播权纠纷案为例,^[18] 原告主张被告在运营网站上擅自发表自己的文章,其委托第三方存取证平台“保全网”对侵权网页进行固定。保全网通过专门软件对目标网页进行域名解析,获取目标网页内容及源代码等涉案信息,将其打包压缩并同步上传至 FACTOM 等区块链平台,获得所存放内容(即涉案网页、源代码和调用信息)的哈希值、^[19] 入链 ID 等。庭审举证时,法庭可以登录 FACTOM 等区块链平台,根据原告提交的哈希值进行搜索,查询该哈希值的存放内容及生成时间等记录,并据此认定侵权事实;^[20] 有关存放内容的证据材料

[12] 此为2019年10月24日习近平在中共中央政治局集体学习“区块链技术发展现状和趋势”时提出的要求。

[13] 参见前引[1],北京市区块链工作专班专家组,第97页。

[14] See Nakamoto Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf>.

[15] “区块”可以进一步分解为“块头”“块身”的大结构以及“区块头信息”“区块高度”等标识符。块头用于链接到前面的块并为区块链数据库提供完整性保证,块身包含了经过验证的、块创建过程中发生的价值交换的所有记录。区块头信息即区块头哈希值,可以唯一、明确地标识一个区块;区块高度是指区块在区块链中的位置,一般创始区块(第一个区块)的高度为0,之后每一个被链接的区块的高度较上一区块高出1。

[16] 公有链是指全世界任何人都可读取、发送交易且能获得有效确认的共识区块链,如比特币区块链;私有链是指其写入权限仅在一个组织控制下的区块链;联盟链是介于公有链与私有链之间、共识过程受到预选节点控制的区块链。

[17] See Angela Guo, *Blockchain Receipts: Patentability and Admissibility in Court*, 16 Chi.-Kent J. Intell. Prop. 440, 442 (2017).

[18] 参见杭州互联网法院(2018)浙0192民初81号民事判决书。

[19] 数据的哈希值是指利用散列函数所产生的,用于校验某一特定长度之数据是否发生变化的特殊数值(如MD5、SHA1、SHA256、SHA512、CRC32值),通常可以针对特定文件计算得出。它可以被理解为任何一段数据的数字指纹,可用于数据完整性方面的验真。只要数值不变,即确定该数据未失真。

[20] 在该案中,法庭根据原告提交的哈希值(c1303aba38f3d134b93026ae65e305266b421273d1303d20a631a919bd9530c)查询到FACTOM区块链的区块高度为103140,并确认该区块高度生成时间为“Friday, August25, 2017, 16:24”,入链ID为“589ef8eaad4bc61837b38bd3dcd4b747ac9fa83b8069c1da05fcc8ee4b0c6”,区块存放的内容为“5f188779155cb6fc2d3822f830256282a464af15d5e9f6af68572533c17a9bea”,存放内容与送检文件的SHA256值一致。

来源及可靠性等问题，亦同时得到解决。^[21]在此次运用区块链技术的证明活动中，完整的证明材料可以被简化为区块链记录与解读性意见两种。

区块链记录，亦称区块链数据、区块链单据，是依靠区块链技术增强真实性的主要数据，用于证明案件中的争议事实；解读性意见是基于“区块”与“链”信息作出的解释、说明，用于辅助前者。在前述案件中，第三方取证平台将获取的涉案网页、源代码等证明材料上链后所形成的存放内容，即属区块链记录，法庭对其进行审查判断的结果和鉴定机构的鉴定意见则为解读性意见。解读性意见还可以呈现为第三方取证平台的技术说明或认证证书、公证机构的公证书或公证保管函、^[22]专家证言、^[23]情况说明以及专业司法人员、专家辅助人的判断等。申言之，区块链记录为主证据，解读性意见为从证据，构成“主—辅”型证据组合。

影响控辩双方利益的最直接因素是对案件争点的认定，故区块链记录能否以及如何用作证据乃根本问题，而解读性意见并无展开独立讨论的意义。一些国家在创新规则时亦仅着眼于区块链记录，普遍将其纳入电子记录进行规则适配。例如，2018年8月美国俄亥俄州修改的统一电子交易法规定，电子记录是指“通过电子手段创制、生成、发送、交流、接收或存储的记录”，“经由区块链技术……获得的记录”属于电子记录。^[24]下文聚焦于如何以区块链记录证明案件事实，仅在必要时述及解读性意见。

当前常见的区块链记录，根据其外在样态可以划分为三种。第一种是基于区块链技术生成的原生型数据。常见者为侦查人员针对利用区块链平台实施诈骗、勒索、洗钱、合同诈骗、集资诈骗、非法吸收公众存款、破坏计算机信息系统、非法获取计算机系统数据、侵犯公民个人信息、组织领导传销活动以及掩饰隐瞒犯罪所得、收益等存在占有或使用非法数字货币情节的多种犯罪，经取证溯源可以获得有关的特殊数据。民事、行政诉讼中亦不乏关于非法数字货币的数据、地址信息、转账记录的证据。例如，在一起民间借贷纠纷案件中，^[25]被告辩称其通过原告手机转账购买了11万余元的以太币，并提交火币网转账记录截图证据，该材料原件即属于区块链生成之证据（此截图属于复制件）。这些数据系在无人工干预的情况下原生于区块链平台，得以在案发过程中、数据形成之际以其技术特性促进防篡改，因此堪称自然意义上的区块链证据。

第二种是基于区块链技术存储的网络数据，其指通过区块链存证平台进行保存或管理而形成的派生型证据。如2018年4月某大学教授涉嫌性丑闻一事，有网友将一封具有影响力的公

[21] 该案实际上进行了双重入链和双重验证。保全网对侵权网页进行固定时，不仅将获取的涉案网页、源代码和调用信息打包压缩同步上传至 FACTOM 区块链，也同步上传至比特币区块链，获得双链中存放内容的哈希值、入链 ID 等。验证时，庭审登录 www.blockchain.com 和 www.btc.com，输入前述交易哈希值查询到区块高度为 482210，出块时间为“2017-08-27 13:31:20”，区块存放的内容为“4661000000192e45c8a0aceda219e436f589902125b359e4db38268d201caf6f195c0c9a8ae4749”，存放内容与送检文件的 SHA256 值一致。

[22] 例如，一起著作权权属、侵权纠纷案件中，有关公证处出具了“电子数据公证保管函”。参见北京互联网法院（2019）京 0491 民初 798 号民事判决书。

[23] 这里的专家证言是广义概念。有论者曾以比特币案件为例，指出交易所程序员、狂热的比特币用户、复制区块链的程序员、数字货币专家或比特币投资者均可作为专家证人，向法庭解释区块链单据的流程、准确性及特别可靠性。参见前引 [17]，Angela Guo 文，第 448 页；Neil Gray & Maxwell J. Eichenberger, *Blockchain: Immutable Ledger, but Admissible Evidence?*, *New York Law Journal*, Dec. 14, 2018, <https://www.law.com/newyorklawjournal/2018/12/14/blockchain-immutable-ledger-but-admissible-evidence>。

[24] *Ohio Rev. Code Ann.* § 1306.01 (West 2019)。

[25] 参见重庆市垫江县人民法院（2020）渝 0231 民初 411 号民事判决书。

公开信存入以太坊区块链,使该信息被保存下来用作证明材料。^[26]基于区块链技术的特点,该公开信自入链之日起即固定于区块链而不会被删改。该公开信即属区块链存储之证据。一般而言,被入链存储的多是各种电子数据,但也可以是各种传统证据的电子化材料。例如,当事人或办案人员对物证拍照或录像后入链,或将书证扫描成PDF文件等入链,其他以电子形式呈现的笔录证据亦可入链。

第三种是基于区块链技术核验的网络数据。例如,在王某某等人诈骗罪案件中,侦查机关向支付宝公司调取王某某支付宝账号的交易信息,并采取区块链存证技术保护电子证据的完整性。详言之,经侦查机关向支付宝公司调证,该公司运用蚂蚁区块链技术将王某某等人的支付宝账户交易流水账单用加密算法上传至“法证链”(一种通过区块链技术提高办案效率的辅助系统),并向侦查机关提供一张含有该电子证据的光盘及一份载有哈希算法、哈希值、时间戳、区块高度等信息的情况说明。庭审中,检察机关通过多媒体示证进行演示,^[27]证明在案电子证据具有真实性。最终,法院认定控方提供的光盘数据合法有效,理由是“支付宝公司出具的光盘内储存内容的hash值与‘法证链’区块链上存放的hash值一致”。^[28]光盘中的支付宝账户交易信息(涉案电子证据)证明了案件事实,而入链的仅是该电子证据的哈希值(作为涉案电子证据未发生篡改的旁证)。入链所形成的区块链记录实乃一种衍生型证据,本文考虑到其重要性称之为“区块链核验之证据”。

可见,区块链生成、存储、核验的证据,均受技术加持而强化了数据的真实性。从技术角度观之,三者的共性在于均采用去中心化的分布式存储技术、多节点共享的读取技术、严格的入链后防篡改技术。区块链记录用作证据的三种样态呈现出类聚特征,故本文将它们合称为“区块链证据”,^[29]意指借助区块链技术生成、存储、核验而来的一切证据。^[30]

(二) 区块链证据的价值阐释

区块链记录用作证据,并非简单地认可新型材料用作证据的地位问题。实践表明,区块链证据在解决重大证明难题与促进司法进步方面,具有独到的价值。

其一,区块链证据是厘清涉众复杂案件事实的最佳证据。2017年,美国特拉华州衡平法院审判都乐食品集团公司股权纠纷一案所遇到的难题,即清楚地说明了这一点。该公司自2013年开始的一次争议股权收购完毕后,持有49,164,415股的股东代表提起了关于涉嫌收购

[26] 该证明材料可以通过四个步骤获取:第一步,任意打开一个ETH区块链浏览网站,如<https://www.etherchain.org>;第二步,在查询框里输入哈希交易码0x2d6a7b0f6adef38423d4c62cd8b6ccb708ddad85da5d3d06756ad4d8a04a6a2,可查询到16进制字符的结果;第三步,搜索一个16进制转UTF8的网站,如<https://www.browserling.com/tools/hex-to-utf8>;第四步,将复制出来的16进制字符粘贴在转UTF8网站中进行解码,最终会得出中英文对照版的“某大公开信”。见https://blog.csdn.net/weixin_30492047/article/details/97975635。

[27] 公诉人举证时的具体做法分为三步:一是获取写入区块链的哈希值。登录“法证链”,通过搜索区块高度锁定特定区块,再对比哈希值、时间戳等信息验证该区块未经修改。二是在工具HashTools中导入在案电子数据文件,并选取与支付宝公司加密原始电子数据时相同的哈希算法SHA256,计算出该电子数据的哈希值。三是进行哈希值对比。将当时写入“法证链”的哈希值与检察机关计算出的电子数据的哈希值进行对比,发现一致的,可以认定在案电子数据与支付宝公司服务器内的原始数据具有同一性。

[28] 参见浙江省绍兴市上虞区人民法院(2019)浙0604刑初486号刑事判决书。

[29] 有学者认为区块链证据仅仅是“通过区块链进行电子数据存证”的结果,甚至认为其就是“区块链存证”。参见前引[10],罗恬瀛文,第65页。

[30] 从更广阔的视野看,尚有其他衍生自区块链技术的证据样态。如与区块链记录相关的APP客户端数据、登录日志、账号、密码、合约订单等,它们可以作为源于区块链技术的延展型证据。考虑到它们同区块链技术的联系很弱,本文对这类证据不予讨论。

欺诈的集体诉讼。^[31] 该公司依法只发行了 36,793,758 股, 即至少有 1200 万股缺少要求结算支付的权利证书。但是, 股东代表对所有主张的权利均拿出了有效证据。该公司未能确定“当时”所有股东, 且委托美国存管信托公司 (DTC) 进行调查亦未能确定有关事实。^[32] 主审该案的法官指出, 现行记账系统已经过时且太复杂, 无法准确及时地跟踪谁是某一份股票的真正所有者以及股东如何在公司决策中行使投票权。^[33] 法官在一份 17 页的备忘录意见书中指出, 该问题的解决之道是区块链技术: “分布式账本技术可以为维护单一、综合的股份所有权账本的多份可流通副本提供一个潜在的技术解决方案”; “有了分布式账本, 像 DTC 这样的集中记账者即无存在的必要……一种单一的分布式账本将允许直连记账”。^[34] 实际上, 纳斯达克等股票交易所已先后开展区块链技术应用, 将上述建议付诸实践。2017 年 7 月, 特拉华州通过了区块链法案, 修改了该州法典的第八章“公司法总则”,^[35] 明确允许在该州注册的公司得于区块链平台上发行和交易股票。^[36] 区块链技术不仅被用于股权投资、证券管理等活动, 也被不断扩展运用于选举投票、文件管理、数据管理、资产管理等活动。

刑事诉讼中也呈现出同样的趋势。例如, 2017 年, 美国联邦第二巡回上诉法院针对暗网“丝绸之路”犯罪的判决载明, 调查人员从被告人乌布利希的笔记本电脑中查获了价值约 1800 万美元的比特币, 并分析了其基于区块链记录的海量交易历史, 以确定其中约 89% 比特币的来源。^[37] 之后, 不同类型犯罪案件中使用区块链记录的情形也有所增多。^[38] 随着当前涉众型经济犯罪形态持续扩增, 运用区块链证据解决证明难题已是大势所趋。

其二, 区块链证据是运用海量异构证据办案的有效方式。涉众型案件的证据特点是有关材料数量繁多、结构冗杂。动辄数以万计的涉案人数、数以亿计的涉案金额, 使得案件办理无法摆脱庞杂的书证、物证、证人证言、笔录等材料, 更难脱离以各类数据为基础开展分析而形成的专业报告。如何保证这些材料来源属实, 是极为棘手的问题。

例如, 2016 年全国各地办理“e 租宝”非法吸收公众存款案件时, 为查清投资人规模及信息, 由公安部组织搭建专门网站 (非法集资案件投资人信息登记平台, ecidcwc.mps.gov.cn) 进行登记, 短短 10 天内涌入了 24 万余名“投资人”。填报信息的准确性难免让人生疑, 相关登记材料亦难以作为呈堂证据。办案机关还从银行调取了 1 万多个账户的信息和几十亿条

[31] *In re Dole Food Co.*, No. 8703-VCL, 2017 Del. Ch. LEXIS 25 (Del. Ch. Feb. 15, 2017), <https://courts.delaware.gov/Opinions/Download.aspx?id=252690>.

[32] 美国存管信托公司系美国清算机构托管信托清算公司 (DTCC) 的分支机构。自 1973 年创建时起, DTC 一直通过簿记对股票所有权进行追踪。

[33] Vice Chancellor J. Travis Laster, *Keynote Speech at the Fall 2016 Meeting of the Council of Institutional Investors: The Block Chain Plunger; Using Technology to Clean Up Proxy Plumbing and Take Back the Vote*, Sept. 29, 2016, p. 14, https://www.cii.org/files/09_29_16_laster_remarks.pdf.

[34] 分布式账本技术常被视为区块链技术, 但实际上, 它是一个比区块链技术更宽泛的相关概念。简言之, 区块链技术只是分布式账本技术中的一种。

[35] An Act to Amend Title 8 of the Delaware Code Relating to the General Corporation Law, Delaware State Senate, 149th General Assembly, Senate Bill No. 69, <https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=25730&legislationTypeId=1&docTypeId=2&legislationName=SB69>.

[36] See Noelle Acheson, *Equity Markets on a Blockchain: Delaware's Potential Impact*, CoinDesk, Jul. 10, 2017, <https://www.coindesk.com/equity-markets-blockchain-delawares-potential-impact>.

[37] *U. S. v. ULBRICHT*, 858 F.3d 71 (2017), <https://www.leagle.com/decision/infco20170531115>.

[38] See *United States v. Costanzo*, 956 F.3d 1088 (2020), <https://www.leagle.com/decision/infco20200417129>; *United States v. Gratkowski*, No. 19-50492, No. 19-50492 (5th Cir. 2020), <https://cases.justia.com/federal/appellate-courts/ca5/19-50492/19-50492-2020-06-30.pdf?ts=1593559812>.

资金交易流水信息,但只能用作办案线索,盖因其无法满足作为定案根据之证据的基本要求。若该办案平台当时采用了区块链技术,则关于投资人的网站登记材料、资金流水信息的真实性疑问将得以消除。基于改进此等做法的考量,2020年,公安部联合银保监会在部分省份上线“资金查控电子证据化系统”,构建基于区块链技术的“(资金查控)证据池”,试行“打印即成证”的新机制。具体来说,每一条资金查控信息被收集后均及时入链存储,确保其可溯源且不发生篡改,从而能够清楚地用于庭审举证质证。如此调取资金数据证据不仅可靠而且高效。海量资金数据可以如此调取,海量的证人证言等证据亦然。

在域外,欧洲正在实施“洛卡德”计划,以搭建“通过区块链技术处理电子化证据的下一代欧洲平台”,“为执法机构、司法当局和私营技术公司提供轻松管理电子证据的工具”。^[39]美国大力推广区块链证据系统(BoE),以解决每一份证据进入保管链后的全程追踪及有效运用问题。^[40]印度尼西亚专家提出“区块链电子证据袋”(B-DEC),以基于以太坊的智能合约方案解决电子证据处理与保存过程的数据完整性管理问题。^[41]这些行动针对的具体对象多种多样,但均展示了以区块链证据应对证据巨量化、异型化问题的可行路径。

其三,区块链证据是提升智慧司法探索水平的重要抓手。在我国,区块链证据的涌现与智慧司法创新是相伴相随的,其率先在互联网法院大量出现即为智慧司法创新的主要场景。自从三家互联网法院的区块链存证系统运行后,办案平台便可自动进行验证。如北京互联网法院的“天平链”平台无需法官介入即可自动核验入链数据,若验证结果证明涉案证据自存证到“天平链”之后未经篡改,即代表其成功通过区块链存证验证。^[42]经调研了解,法官看到的“天平链”平台验证报告的内容非常丰富,包括当事人姓名、手机号、身份证号、存证名称、存证编号、存证时间、存证内容、验证结果等,可以确定整个业务行为进展的过程等。此外,北京互联网法院自2019年10月17日开展由智能合约自动发起执行立案的全国第一案之后,区块链技术被嵌入审判执行工作,完成智能合约的线上节点部署,并通过当事人的确认触发立案、调解、执行动作,实现“一键立案”“一键转调”“一键执行”等智能应用。此皆为区块链技术推动司法活动智能化提级的例证。

[39] European Commission, *Lawful Evidence Collecting & Continuity Platform Development*, <https://locard.eu/>.

[40] See Derick Anderes et al., *The Use of Blockchain within Evidence Management Systems*, <https://f.hubspotusercontent10.net/hubfs/5260862/Blockchain%20of%20Evidence%20FINAL%20DRAFT.pdf>.

[41] See Eko Yudianto, Yudi Prayudi & Bambang Sugiantoro, *B-DEC: Digital Evidence Cabinet Based on Blockchain for Evidence Management*, 181 (45) *International Journal of Computer Applications* 22 - 29 (2019).

[42] 经实测,验证成功时将显示“当前文件与区块链存证文件一致”,验证失败时显示“当前文件与区块链存证文件不一致”。以“司法上链第一案”蓝牛仔影像(北京)有限公司与华创汇才投资管理(北京)有限公司著作权权属、侵权纠纷案为例,区块链证据的运用通常分为三个步骤:(1)事前存证。原告向“版权家”(第三方存证平台)提出关于一张数码照片的存证申请,获得电子数据存证证书,经过其可信存证系统“版权链”进行保管。“版权链”通过跨链操作将其区块的摘要数据在“天平链”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”上的存证编号及其反映的文件。(2)事中监测。原告通过版权大数据监测,发现涉案照片被侵权,即收集相关侵权图片线索,将侵权线索存证至“版权链”,“版权链”通过跨链操作将其区块的摘要数据在“天平链”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”上的存证编号及其反映的文件。(3)事后验证。当诉讼发生时,原告通过电子诉讼平台进行网上立案,同时提交起诉状、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。法官即可凭借“天平链”验证结果对电子证据予以认可。以上内容来源于北京互联网法院(2019)京0491民初724号民事判决书以及该案办案人员的情况介绍。

三、法律及规范对区块链证据的理性认可

前文的一个基础论断是，在现行证据规则体系下，区块链证据并不构成同现行八种法定证据形式相并列的新的证据形式。申言之，区块链证据仅是产生自“区块链+证据”创新的新样态。在此认识框架下，法律及规范对区块链证据的认可应当坚守审慎立场，遵循两项基本原则：平等性对待和差别性归位。

（一）平等性对待

所谓平等性对待，是指法律及规范对区块链证据样态应施以等同于现有法定证据形式之处遇，对区块链证据的具体部分亦应予以同等处遇，绝不因其萌生于新技术环境而有所排斥或偏重。此原则在早年各种新的“数据电文”诞生时，即被反复申明。如1996年联合国国际贸易法委员会《电子商务示范法》第5条规定：“不得仅仅以某项信息采用数据电文形式为理由而否定其法律效力、有效性或可执行性。”^[43]该规定为许多国家的法律所借鉴，如2004年我国制定电子签名法，其第7条规定：“数据电文不得仅因为其是以电子、光学、磁或者类似手段生成、发送、接收或者储存的而被拒绝作为证据使用。”

在美国，一些州作为区块链证据规则的先行者，^[44]主要采取两种方式强调平等性对待原则。一是单独规定区块链记录的证据地位。如2019年华盛顿州关于承认分布式记账技术的有效性的法律，其规定“不得仅仅以电子记录系使用分布式记账技术生成、交流、接收或存储为由，否定其法律效力、有效性或可执行性”。^[45]二是与智能合约、电子签名等一起，一并规定其法律效力。如2020年1月生效的伊利诺伊州区块链技术法规定，“不得仅仅因为智能合约、记录或签名是由区块链创建、存储或验证的，而否认其法律效力或可执行性”；“在诉讼中不得排除基于区块链创建、存储或验证的智能合约、记录或签名的证据”；“若法律要求提供经签名材料的，则提交以电子方式记录于区块链或区块链证据的签名数据，以核实旨在提供签名者的意图，同样满足该项条件”。^[46]亚利桑那州、纽约州、俄亥俄州的相关法案、法律也作了此类调整。^[47]

欧洲部分国家同样确认了区块链记录及其具体部分的平等证据地位。如2019年，意大利议会通过第12/2019号法律，确认智能合约和分布式账本技术在法律上的有效性。该法规定，

[43] UNCITRAL, Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, Article 5 “legal recognition of data messages”, p. 5.

[44] See Shelagh Dolan, *How the Laws & Regulations Affecting Blockchain Technology and Cryptocurrencies, Like Bitcoin, Can Impact Its Adoption*, Business Insider, Mar. 3, 2020, <https://www.businessinsider.in/finance/news/how-the-laws-regulations-affecting-blockchain-technology-and-cryptocurrencies-like-bitcoin-can-impact-its-adoption/article-show/74464680.cms>.

[45] Act relating to Recognizing the Validity of Distributed Ledger Technology of Washington, Substitute Senate Bill 5638, 2019.

[46] Blockchain Technology Act of Illinois, H. B. 3575, 2020.

[47] 2017年3月，亚利桑那州通过增加关于电子交易新章节的方式，修订了该州的《修订制定法》。依照新增的条文，通过区块链进行的签署行为被视为满足形式要求的、合格的电子签名，通过区块链获得的记录、合同被视为满足形式要求的、合格的记录；商业活动中可以使用智能合约，不得仅仅因为合同中包含智能合约条款而否定其法律效力、有效性或可执行性。2019年1月、3月，纽约州参议院第1683号、第4142号法案对州技术法律中的电子签名与文件法提出了修改建议，这两部法案包含确认可以通过区块链进行签名、签约的规定，亦包含确认智能合约有效性的规定。在俄亥俄州，参议院第300号法案于2018年5月被提交讨论，该法案建议承认智能合约具有完全的法律效力和可执行性。

基于分布式账本技术存储的电子文件具有同欧盟《电子身份认证与签名条例》规定的加盖电子时间戳一样的法律效力。欧盟《电子身份认证与签名条例》第41条第1项规定：“在法律程序中，不得仅仅因为电子时间戳系电子形式、或其不满足合格的电子时间戳之要求为由，否定其法律效力和作为证据的可采性。”〔48〕

相比欧美，我国在区块链证据方面的实践探索更显超前。在我国，国家力量主导了区块链存证的多项重大试验，特别是以互联网法院为代表的部分司法机关搭建了专门的司法区块链平台并得到广泛运用。当下，我国不仅有丰富的区块链生成、存储之证据（这一部分与欧美趋同），更有大体量的区块链核验之证据（这一部分在欧美未见新闻报道，亦未经调查发现）；不仅有电子数据的入链，也有电子数据校验值的入链、传统证据电子化之后的入链。如此情势下，我国既要克服部分司法人员因认识不足而规避乃至歧视区块链证据或其具体部分的问题，更要警惕超越合理限度高看区块链证据或其具体部分的问题。对于前一点，可以借鉴欧美经验，通过确立平等性对待原则消解对区块链证据的低看；对于后一点，则要因势利导。

近年来，我国证据规范建设中高看区块链证据或其具体部分的现象，已初现端倪。一些司法解释违反技术中立原则，赋予区块链证据或其具体部分以超级地位。如“互联网法院审理案件规定”第11条第2款，其不仅将“区块链”等技术手段单列规定，而且明确规定法院“应当”确认其真实性。然而，区块链技术、区块链平台并非完美无缺，此般规定显然在逻辑上无法自洽。更突出的问题是，明文要求法院“应当”确认受特定技术影响的相关证据，于法理不通，于实践不妥。该解释的制定者还申明，以区块链证据消减在线诉讼中对公证书证据的需求，乃当前最高司法机关制定司法解释所追求的方向。〔49〕此说法隐含着将区块链证据等同于甚至超越于公证书证据（一种传统上认为具有优先地位的证据）的意思。然而，与公证书证据占优先地位具有法理与观念基础相比，区块链证据以后来者身份“空降”代位，尤其显得突兀。“在线诉讼规则”单列出关于“区块链证据”的四个条文，其合理性论证同样不足，表现出人为拔高区块链证据地位的倾向。

学术界也出现了高看区块链证据之具体部分的观点，即主张对区块链证据进行拆分并赋予不同等级的信任值。例如，有人根据公有链、私有链和联盟链的分类，提出了基于司法联盟链〔50〕的区块链证据相比基于其他链的区块链证据具有更好的真实性保障的观点，因为“司法联盟链的主要特征是链上节点包含司法机关、公证机关，既有技术安全性的支撑，也有国家与机构信誉的背书”。其明确建议，对基于司法联盟链的区块链证据，“可以设定较为简单的认定标准”；对基于商业联盟链的区块链证据，“设置较为严格的审查认定规则”。〔51〕此种论断的推理脉络过于简单化，存在滑向形式主义审查的危险，亦属于对平等性对待原则的违背。

对区块链证据或其具体部分高看一眼，只是一种臆断。笔者对北京互联网法院一线法官进

〔48〕 eIDAS Regulation.

〔49〕 “互联网法院案件在线审理和大量证据在线的特征，客观上要求打破通过公证程序认定真实性的单一途径，通过技术手段和相关配套机制对电子数据真实性作实质性认定”。胡仕浩、何帆、李承运：《〈关于互联网法院审理案件若干问题的规定〉的理解与适用》，《人民司法（应用）》2018年第28期，第27页。

〔50〕 所谓司法联盟链，是以法院为中心搭建，使用区块链技术将公证机构、CA/RA机构、司法鉴定中心以及法院连接在一起的联盟链。参见崔世群：《区块链证据真实性问题研究》，《经贸法律评论》2021年第3期，第145页。

〔51〕 参见段陆平、罗恬瀚：《在线诉讼区块链证据规则的理论逻辑与制度体系》，《民主与法制时报》2021年7月22日第6版。

行调研发现，目前几乎所有当事人均未对纳入“天平链”的网络数据提出过真实性异议，法官也基本上不作区块链证据是否属实的审查。这表明，区块链证据在我国的实践中一定程度上被神化了。若证据规范建设中再抛出缺乏正当性的高看区块链证据的专门规定，更将加剧神化区块链证据的不良倾向。对此，应回归同等对待区块链证据与非区块链证据，同等看待区块链证据之具体部分的基点。

（二）差别性归位

区块链证据系由各种网络数据产生或汇聚于区块链系统或平台而出现。当前区块链技术还存在特定发展阶段的缺陷，突出的表现是链上节点的数据容量有限。有专业团队研究指出，“区块链的不足在于适合存储体量小的数据，比如业务流程中产生的数据，采集过程中的案情、记录，鉴定报告等”。^[52]随着区块链技术不断取得突破，链上节点的数据容量定会持续增长，各种证据（或其复制件）呈现于区块链不会遇到无法跨越的技术障碍。其实，我国已开展证据复制件、数据哈希值入链的试验，现行八种法定证据形式均有成于链或存入链的情况。因此，运用区块链证据的另一要义在于对其进行差别性归位。

确立该原则的理由之一是，区块链证据并非一种独立的证据形式，今后亦无将其增列为一种法定证据形式的必要。我国法律规定的“视听资料、电子数据”属于电子形式，可以产生、存储于区块链；“物证”“书证”“证人证言”“被害人陈述”“犯罪嫌疑人、被告人供述和辩解”“鉴定意见”“勘验、检查、辨认、侦查实验等笔录”虽一般不属于电子形式，但亦可以先行电子化而后存入区块链。从这个意义上讲，区块链证据的实质是现有法定证据形式（或其复制件、衍生件）的区块链化。^[53]

确立该原则的理由之二是，区块链证据可能是证据原件（原始证据），也可能是证据复制件（派生证据），甚至可能是与原件、复制件相关的证据转化件（衍生证据）。这就意味着，审查运用区块链证据时需要判断其是原件、复制件还是转化件，要接受原件规则、最佳证据规则或证据转化规则的规制。基于此，实践中对区块链证据要作具体分析、具体归类，判断其是否属于原件等。此即差别性归位的涵义。

我国有学者讨论过将书证转化为区块链证据的问题，^[54]在此亦以通过区块链技术签署合同为例加以补充说明。通过区块链技术签署合同，一种做法是合同双方对纸面合同签章后将其备份、存入区块链平台，另一种做法是合同双方在区块链平台直接签署智能合约式的合同。在前一情形下，入链形成的是区块链存储之证据，该证据同时也是“书证”，且属于典型的复制件。在后一情形下，链中内生的是区块链生成之证据，该证据同时也是“电子数据”，且属于典型的原件。照此判断结果，这两种情形下的区块链证据要分别接受书证、复制件之一般规则与电子证据、原件之一般规则的约束。至于因其涉及区块链技术而是否需要接受特殊规则的约束，这是要额外考虑的事情，具体取决于是否增设了相关的特殊规则。

其实，贯彻差别性归位原则乃国际共识。该原则决定了各国不必另起炉灶开展区块链证据规则建设，而是在认可现有规则可用的基础上进行必要的调整或补充。例如在英美法系，区块

[52] 曾超等：《公检法基于区块链和大数据共建证据链》，《信息安全与通信保密》2021年第1期，第44页。

[53] 为避免将区块链证据仅仅理解为电子证据、电子数据之变体，笔者在前文关于区块链证据的定义中刻意选择“网络数据”作为关键词。“网络数据”应作广义理解，既包括自然生成的网络数据，也包括其他证据转化为电子形式而生成的网络数据。

[54] 参见前引〔10〕，罗恬漩文，第71页。

链生成、存储之证据要分别通过鉴真规则、传闻规则的检验，^[55]就像计算机生成、存储之证据要分别通过鉴真规则、传闻规则的检验一样。^[56]至于特殊规则的部分该如何设计，则需要考虑区块链证据的特殊性。

四、区块链证据的真实性原理及规则

从证据法理看，区块链证据运用于司法的核心问题是如何审查判断其可采性和证明力。从技术形态看，区块链证据主要在真实性方面独具风格。其制度建设应当聚焦于真实性问题，在客观规律的基础上进行证据规则的构建。

（一）区块链证据真实性增强的原理

国内有论者提出，电子证据的真实性包括“电子证据载体的真实性”“电子数据的真实性”和“电子证据内容的真实性”三个层面；^[57]亦有论者据此将区块链证据的真实性区分为“载体真实性、数据真实性、内容真实性”三层含义。^[58]这种三分法经不起细节上的推敲，划分结果亦无实际意义。^[59]从司法实践观之，案件中证据的真实性问题肯定是具象的，“司法只需要解决控辩双方对涉案电子证据的哪一种说法更可信的问题”。^[60]此乃电子证据的理性真实观，其同样适用于区块链证据。以此为基点，需要先透析区块链证据在真实性方面的客观机理。

1. 数据入链后防篡改的现象与定律

区块链技术的哈希校验、时间锁定与节点印证，是强力防范数据入链后失真的三大支点。所谓哈希校验，是通过数据的哈希值（完整性校验值）保障数据不被篡改的方法。在实践中，哈希校验被广泛运用于司法鉴定、刑事侦查、民事调查、纪检监察等取证活动，成为各种电子取证措施的技术标配。这一方法在区块链证据的保真上被再度发扬光大。一般要求在数据入链时计算其哈希值，^[61]事后在区块链平台的节点查询哈希值予以验真。如在前文提及的侵害作品信息网络传播权纠纷案中，法院、鉴定机构均查询到区块存放内容在 FACTOM 区块链、比特币区块链上的哈希值，并以此确认“存放内容与送检文件 SHA256 值一致”。^[62]

所谓时间锁定，是赋予入链数据以各种权威时间戳机构签发的具有法律效力的电子凭证。它保证数据在特定时刻点已经客观存在，以进行数据时间方面的验真。如在前文提及的侵害作品信息网络传播权纠纷案中，FACTOM 区块链中有关区块高度的生成时间为“Friday, August 25, 2017, 16:24”，比特币区块链中有关区块高度的生成时间为“2017-08-27 13:31:20”。它们反映了不同的入链时间，意味着数据分别于这两个时刻点入链，作为其不可能发生改变的起

[55] See Alex Ashrafi, *Blockchain as Evidence: How Will It Get into Court?*, 2019, <https://www.legaltechcenter.openum.ca/files/sites/159/2019/10/Blockchain-as-Evidence.pdf>.

[56] *Lorraine v. Markel Am. Ins. Co.*, 241 F. R. D. 534, 578 (D. Md. 2007).

[57] 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》，《法学研究》2018年第4期，第123页。

[58] 参见段莉琼、吴博雅：《区块链证据的真实性认定困境与规则重构》，《法律适用》2020年第19期，第149页。

[59] 如区块链证据并不存在一般意义上的载体，其数据与内容难以区隔等。

[60] 刘品新：《论电子证据的理性真实观》，《法商研究》2018年第4期，第65页。

[61] 在仅仅入链对应数据哈希值的情况下，通常做法是对该数据所对应的“文件名称+哈希值”计算新的哈希值之后再入链。

[62] 参见杭州互联网法院（2018）浙0192民初81号民事判决书。

算点。若合并考虑，可以认为有关数据在较早时刻点“Friday, August 25, 2017, 16:24”已经被固定下来。

所谓节点印证，是指入链网络数据是分布式存储的，当各个节点完成记录时，亦同步验证了其他节点记录结果的正确性。若趋近于全节点均同步认定有关记录正确时，或者所有参与记录节点的比对结果一致，目标数据才被允许写入区块，并在盖上时间戳后生成区块数据，然后通过分布式传播发送给各个节点实现分布式存储。司法实践即依据此特点进行数据内容方面的验真。如在前文提及的侵害作品信息网络传播权纠纷案中，FACTOM 区块链中各个节点（如鉴定机构节点）均可查询到入链数据。此外，假如个别节点记录的数据被篡改，则将因其与该系统大多数节点不一致，而被检测出来并被自动纠正。这种节点印证构成一种事实上的证据完整保管链。

值得注意的是，区块链证据的保真范围具有时间段上的限制，即其保真仅指向数据入链后。因为入链前数据与区块链技术无涉，入链前数据的真假问题同一般证据并无二致。而数据一旦入链，其真实性即受哈希校验、时间锁定、节点印证等支点的保障。总而言之，入链后数据真实性有保障，是关于区块链证据真实性的第一定律。

该定律对于区块链生成、存储与核验之证据等样态均适用，但影响程度并不相同，因其在数据入链时刻点同证据形成时刻点的关系上存在差异。具体来说，区块链生成之证据的数据入链时间是案发过程中、网络数据生成时，区块链技术足以确保其整个生命周期的真实性。^[63] 区块链核验之证据的数据入链时间是证据提取过程中、网络数据校验后，区块链技术仅能确保其部分生命周期的真实性。当然，实践中诉辩双方对证据真实性提出的争议，多来自证据提取后的保管阶段，即取证之后，可见区块链技术对于区块链核验之证据所涉数据真实性保障有实际意义。区块链存储之证据的情况则介于二者之间，其数据入链时间可以在证据保全过程中、网络数据校验后，也可以是案发过程中、网络数据生成时。相应地，区块链技术对其真实性的保障，也是两分的。

表 1 数据入链后真实性的类型化分析

		区块链生成之证据	区块链存储之证据	区块链核验之证据
数据防篡改的共同点		以哈希校验、时间锁定、节点印证等技术特性保障数据入链后防篡改		
数据防篡改的差异点	入链的时刻点	证据生成时	取证时或取证后	取证之后
	入链与数据生命周期的关系	入链覆盖数据的全生命周期	入链覆盖数据的全生命周期或后期保存阶段	入链仅覆盖数据的后期保存阶段
	入链对真实性的保障	全程阶段的真实性保障	全程或部分阶段的真实性保障	部分阶段的真实性保障

表 1 说明，入链时刻点是可以尽量前移的，即数据入链的时刻点可以等同于证据生成的时刻点，或者无限接近证据生成的时刻点。例如，在加密数字货币、智能合约等场景下，网络数据实际上是自生成之际即自动同步入链。又如，在第三方开展数据存证的场景下，该区块链平

[63] 就区块链生成之证据而言，其入链的内容是在区块链系统内自动生成的原始数据，数据生成时间即入链时间，因此不存在入链前数据被篡改之虞。

台在网络数据生成之际即完成入链任务。在这两种情况下，数据入链的时刻点逼近证据生成的时刻点。基于此，“入链后数据真实性有保障”定律就衍生出一条亚定律——数据同步入链亦保真。

2. 数据入链前的真实性问题与定律

审查入链前数据是否属实的问题，主要针对存在数据入链前阶段的区块链存储、核验之证据。就区块链存储之证据而言，因其入链行为系于数据生成时由人工完成，其入链时间晚于数据生成时间，故存在入链前数据遭篡改之虞。对此，应对其真实性的三个主要影响因素有所认识：一是入链数据同原始数据是否同一。这涉及区块链证据的原件问题，^{〔64〕}特别是能否保证入链数据内容上的完整性。二是入链时间同数据生成时间的间隔。经验告诉我们，数据被篡改的可能性与其生成后进行入链管理的时长成正相关关系。从数据生成到入链管理，其间的时长越短，数据遭篡改的可能性就越小（或者说对其加以篡改的难度越大）。有观点指出，“目前司法实践中，取证行为尚无法做到证据固定后即时提交，往往会存在一定的时间差，但时间差应当在一个合理的期限内”。^{〔65〕}三是入链次数的多寡。仅完成一次入链的，较难让人相信数据未被篡改；就同一事件进行系列数据多次入链的，则能消除数据造假的疑虑。比如，当事人通过区块链技术签订合同时，将要约邀请、要约、承诺甚至履约行为的相关记录接续入链，能增强数据的可信度。

表2 数据入链前真实性的类型化分析

		区块链生成之证据	区块链存储之证据	区块链核验之证据
是否存在数据入链前阶段		否	是/否	是
入链的内容		/	作为证据的数据	作为证据之数据的哈希值
哈希计算中造假的可能性		/	较小	较大
入链前数据真实性的影响因素	个性因素	/	是否将原始数据入链	是否将保证原始数据不变的哈希值入链
	共性因素	/	入链数据是否等同于原始数据，或者是否固定了原始数据；入链时间与证据生成时间的间隔；入链次数是一次还是多次	

就区块链核验之证据而言，其入链系在证据材料生成之后，且部分证据材料须先行电子化，入链的数据肯定是复制件或衍生件。考虑到区块链核验之证据所入链的哈希值能否保证有关证据材料的原始信息不发生变化，除了前述后两项因素外，还应当重点关注能否有效固定网络数据及其哈希值。从实践看，针对网络数据的哪些版本、何时计算哈希值以及计算几次哈希值等，均会对可能入链数据的真实性产生影响。比如，当事人在电子商务交易中仅将电子邮件合同文本、PDF文件合同文本的哈希值存入区块链存证系统，则该区块链核验之证据遭受真实性质疑的程度，取决于先前是否计算了对诉辩双方具有法律意义的电子邮件合同、PDF文件合

〔64〕 参见前引〔7〕，刘品新文，第26页。

〔65〕 童丰：《公证介入区块链技术司法运用体系初探——从杭州互联网法院区块链存证第一案谈起》，《中国公证》2018年第9期，第63页。

同的哈希值，也取决于其入链内容、时间及次数等。

入链前数据真实性可优化，是关于区块链证据真实性的第二定律。优化的具体方法包括：（1）尽可能缩短数据入链前阶段。若能将入链时间压缩到一个合理的时间内，使其不存在被造假的可能，即可在很大程度上保障入链前数据的真实性。所谓“合理的时间”，指符合业务习惯、不给造假提供可能性机会的一个时间段。美国《联邦证据规则》第803（6）条在解释“正常业务记录例外”规则时使用的经典表述是，“记录形成之际或之后不久”。^[66]我国学者提出，“区块链最典型的存证思路是从数据生命周期开始即介入，即便是碎片化的数据，在其生成时也实现上链固定，同时实时地传送到公证、鉴定、审计或仲裁等机构的服务器。”^[67]这是有道理的。笔者建议，在互联网法院或其他法院开展哈希值入链存证的情况下，司法存证平台要在有关主体对数据计算哈希值之后即刻入链，以最大程度促使入链时刻点接近证据生成时刻点。（2）尽可能用机器取代人工进行数据入链。2018年11月美国国际战略研究中心发布的一份专门报告，提出了这一方案。^[68]该报告举例说，在医疗数据入链存储的情况下，由机器负责编制数据输入能够解决入链数据自始不准确或有欺诈的问题。（3）尽可能进行多维多次数据入链。如果当事人将数据内容、数据属性、数据痕迹等信息入链，或者当事人持续进行数据入链，则可促进对入链前数据真实性作出综合认定。

（二）区块链证据真实性规则的改进

区块链证据在真实性方面存在的两大独特定律，为完善其真实性规则奠定了各国相通的技术基础。与之对应，各国现有的证据规则，特别是关于电子证据真实性的规则，构成了完善区块链证据真实性规则的制度基础。客观审视中外区块链证据真实性规则建设，特别是检讨我国“在线诉讼规则”新设条文的不足，挖掘美国部分州之做法可资借鉴的经验，是推动我国有效改进区块链证据真实性规则的认识基础。

1. 对中美区块链证据真实性规则的评析

中美两国开展区块链证据真实性规则建设均系刚起步，且呈现出守成与创新兼顾的特点。一方面，中美均将关于电子证据真实性的现行规则普遍适用于区块链证据。在美国，“区块链记录属于更广泛的‘电子证据’范畴”。^[69]实践中，普通电子证据可以适用知情人作证、^[70]校验值验证、^[71]电子记录验证、^[72]司法认知^[73]等方法或规则，这些方法或规则亦完全可用于区块链证据。在我国，关于电子证据真实性的代表性规则同样适用于区块链证据。例如，2019年《最高人民法院关于民事诉讼证据的若干规定》（以下简称“民事诉讼证据规定”）第93条、第94条（可合称为“电子证据真实性专条”）确立了审查判断电子证据的推理性标准、推定性标准和认知性标准“三合一”体系，^[74]实践中对区块链记录完全可以按照上述条

[66] Fed. R. Evid. 803 (6) (A), <https://www.rulesofevidence.org/>.

[67] 伊然、董学敏：《互联网审判中区块链存证技术的应用进路》，《人民司法（应用）》2020年第31期，第15页。

[68] See Kati Suominen et al., *Harnessing Blockchain for American Business and Prosperity: 10 Use Cases, 10 Big Questions, 5 Solutions*, Center for Strategic and International Studies, 2018, pp. 15 - 16.

[69] See Lemieux Victoria, *Blockchain for Recordkeeping: Help or Hype?*, 2016, http://blogs.ubc.ca/recordsinthechain/files/2018/06/FinalReport_Volume1.pdf.

[70] 由了解区块链技术的人向法庭进行解释。Fed. R. Evid., 901 (b) (1).

[71] 通过完整性校验值等公认技术手段验证电子证据的真实性。Fed. R. Evid., 902 (13).

[72] 电子证据的真实性得到由电子程序或系统产生的、经证实的记录的验证。Fed. R. Evid., 902 (13).

[73] 法官对区块链证据（如虚拟货币）进行直接确认。Fed. R. Evid., 201.

[74] 参见刘品新：《论电子证据的真实性标准》，《社会科学辑刊》2021年第1期，第68页。

文列举的情形,作出“于己不利的推定”“源于中立第三方平台的推定”“正常业务记录的推定”“档案方式保管的推定”“遵从约定的推定”等。而且,以上推定对区块链证据通常是可以多项共用的。同理,我国实行的“视为电子数据原件”规则亦可适用于区块链证据。^[75]另一方面,美国联邦法律和一些州的法律针对鉴真规则、最佳证据规则与推定规则,作了面向区块链证据的修补;最高人民法院亦在“在线诉讼规则”中推出了“区块链证据真实性专条”(第16条至第19条)。

在洞悉中美做法之共性的同时,更应当清醒地认识到我国所为之应对的局限性。“区块链证据真实性专条”由“在线诉讼规则”中四个相互联系的条文构成(表3)。严格说,这一条文体系指向的仅仅是“通过区块链技术存储校验值或核验的电子数据”,对应的主要是区块链核验之证据,其虽然可以扩大覆盖至区块链存储之证据,但与体量更大的区块链生成之证据着实无关。

表3 “区块链证据真实性专条”解析

条文序号	针对的情形	关于真实性判断方法的表述	基本特点
第16条		经技术核验一致的,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。	(1) 属于软性指引,而非硬性规则; (2) 主要属于程序性规范,缺少实体性规范; (3) 带有技术性、经验性色彩,法学理论支撑不够。
第17条	入链后的真实性	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。	
第18条	入链前的真实性	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。	
第19条	以上两种情形	可以根据当事人申请或者依职权,委托鉴定区块链技术存储电子数据的真实性,或者调取其他相关证据进行核对。	

除了覆盖范围偏窄外,“区块链证据真实性专条”还存在一些明显的不足。其一,同既有证据规则脱节。区块链证据的真实性如何判断,离不开对既有证据规则(特别是“电子证据真实性专条”等规则)的调整与补充。而“区块链证据真实性专条”中,除了第16条带有一点传统证据规则(主要是推定规则)的意味外,第17条至第19条均虚而不实。它们只是告诉司法人员应当或可以干什么,而未附随任何规范后果。换言之,它们只具有宣示意义,而无实质效能。其二,经不起形式逻辑的推敲。“区块链证据真实性专条”的最大创举是将区块链

[75] “民事诉讼证据规定”第15条第2款规定:“电子数据的制作人制作的与原件一致的副本,或者直接来源于电子数据的打印件或其他可以显示、识别的输出介质,视为电子数据的原件。”该款规定显然可以用于解决入链者是否为原始数据的争议。

证据的真实性问题区分为入链前后，并机械地分别作出规定。这一处理是不妥当的。且不论实践中存在“链中链”“链外链”“复合链”等复杂情况，从而难以将区块链证据的真实性截然分为入链前后两个阶段，仅论其针对区块链记录入链前真实性设置专门规则的做法，实属匪夷所思。入链前的记录可以呈现为一切法定证据形式，与区块链技术并无关系，怎么会被纳入区块链证据真实性规则？如此设计，第18条所表达的内容就只能是交由法院结合各种情况进行“综合判断”。如此规定，又有何实际价值？其三，对法律要素与技术要素的配置存在错位。第17条针对区块链记录入链后的真实性问题，明确规定法院应结合多种因素作出判断，既包括“存证平台是否符合国家有关规定”，“当事人与存证平台是否存在利害关系”，“利用技术手段不当干预取证、存证过程”等可能导致违法或不当存取证的法律要素，也包括“存证平台的信息系统是否符合清洁性等标准”，“存证技术和过程是否符合信息验证等要求”等技术要素。这样的规定似是而非，因为法律要素指向的是证据的合法性而非真实性问题，而技术要素的判断则是司法人员难有作为的。

与此相对，美国的区块链证据真实性规则虽然受制于实践创新不足，但不乏可圈可点之处。这突出表现为一些州的立法通过拓展“自我鉴真”“业务记录例外的推定”及“推定范围”等规则进行应对。早在2016年6月，佛蒙特州通过了《关于多样性经济发展的法律》，专章规定有关确认区块链记录有效性及法庭上可采性的条款。该法规定，若以电子方式登记于区块链的电子记录得到适格者经书面声明的宣誓支持，则其是自我鉴真的；有关的书面声明要表明其本人制作了该书面声明，表明该电子记录进入区块链的日期、时刻，表明该电子记录被保管在区块链中是一种正常业务活动，并表明该电子记录按照正常业务活动处理符合习惯做法。当然，该项推定（自我鉴真）并不表明案件事实或记录的内容具有真实性、有效性或合法性。该法与《佛蒙特州证据规则》的效力规定相同，均确认了以区块链方式存储的电子记录在庭审或听证中具有可采性。2019年9月，弗吉尼亚州将名为“商业记录；登记于区块链的、自我鉴真的电子文件”的条款建议作为第2415号法案提交给州众议院。该法案规定，“在任何民事诉讼中，如果在区块链上以电子方式登记的商业记录是实质性的、可采的，则应当推定该记录是自我鉴真的，不再要求外在证据证明其真实性”。^[76]该法案确立的推定规则与佛蒙特州《关于多样性经济发展的法律》中规定的推定规则相同，特别是在推定记录的真实性、记录的日期和时刻以及记录的制作者方面。纽约、加利福尼亚等州亦模仿佛蒙特州《关于多样性经济发展的法律》，颁行了类似规定。^[77]

综观上述美国各州立法，不难发现其区块链证据真实性规则的优势在于实质有用，而这归因于三项共识。一是规则建设的重点是入链后数据的真实性，入链前的记录不在规则建设的范围内。二是立足于法律上的真实性。美国各州的区块链证据适用“业务记录例外的推定”等规则，这表明司法实践对区块链证据并不追求技术上百分之百不可造假意义上的真实性。这对于我国在区块链证据真实性问题上坚持理性真实观应有所启发，即使用区块链证据只需要追求

[76] House Bill NO. 2415 (Business Records; Electronically Registered on a Blockchain Self-authenticating Document). A BILL to amend the Code of Virginia by adding a section numbered 8.01 - 390.4, relating to business records electronically registered on a blockchain self-authenticating (2019).

[77] See Joanna Caytas, *Blockchain in the U. S. Regulatory Setting: Evidentiary Use in Vermont, Delaware, and Elsewhere*, Columbia Science & Technology Law Review (May 30, 2017), <https://ssrn.com/abstract=2988363>.

“在具体案件中达到法律标准的真实”。^[78] 三是以侧面认定机制为方向。任何证据的审查判断规则均可从正侧两面切入,前者是正面规定综合性的审查判断要素或标准,后者是侧面规定确认证据是否属实的方法。在普通司法人员还难以胜任正面认定区块链证据真伪的今天,先行构建侧面认定机制不失为一种更加可行的方案。

2. 我国区块链证据真实性规则的完善

截至目前,我国司法机关不仅作出了数量可观的、基于区块链证据的司法裁判,而且是区块链证据平台的主导者或主要参与者。司法机关设计、开发和运营着一些专门的区块链证据平台,也引导公证机构、鉴定机构、社会调解组织、行政执法机关等参与其中,构成了一个庞大的生态系统。这为我国构建足够刚性的区块链证据真实性规则,提供了更为丰富的实践资源。

表4 区块链证据样态中影响真实性规则的因素

	区块链生成之证据	区块链存储之证据	区块链核验之证据
提供区块链服务的主体	网络服务提供者(可以是当事人)	第三方网络服务提供者(不包括当事人)	法院等办案部门
参与区块链服务的主体	当事人、案外人等	当事人、案外人、商业服务机构、法律服务机构等	
出具关于区块链证据的解读性意见的方式	当事人陈述、证人证言等	当事人陈述、证人证言、第三方存证报告、档案管理报告、公证书、鉴定意见、行政执法部门审查意见、司法部门审查意见、侦查机关情况说明等	

由表4可知,多元主体为区块链证据是否属实提供了多元证明方式。不仅可以传唤当事人、证人、专家辅助人、第三方存取证平台、档案部门出庭作证,亦允许举证方提交公证书、鉴定意见、行政执法部门审查意见、司法部门审查意见、侦查机关情况说明等进行证明。这为我国设置具体的推定、司法认知机制及建立可操作性强的规则打下了基础。

关于区块链证据真实性推定机制的设置,“电子证据真实性专条”已经明确了“正常业务记录的推定”等若干推定情形,涵盖并超出了美国部分州所采取的“业务记录例外的推定”规则。是故,我国关于区块链证据真实性推定的规则建设,主要是将区块链证据同“电子证据真实性专条”中的推定规则相勾连。至于“推定区块链证据属实”应当是指什么含义,我国亦可借鉴域外做法来加以明确。如美国佛蒙特州《关于多样性经济发展的法律》为区块链记录规定了推定规则:(1)该记录被推定是真实的;(2)该记录被存入区块链的某个日期及具体时刻被推定为实际日期及时刻;(3)区块(链)的建立者被推定为记录者;等等。对此,当事人可以通过提交证据证明“区块链中所述日期的推定事实、记录时间或身份不属实”等,进行反驳。^[79]再如欧盟《电子身份认证与签名条例》第41(1)条规定:“仅仅针对合格的电子时间戳可以进行推定,推定该数据标示的日期、时刻是准确的,推定该数据截至所标示的日期、时刻是完整的”,^[80]即“推定区块链证据属实”有时仅系对形式真实性的确认。

结合前述关于数据入链的两条定律和既有推定规则,本文分别针对区块链生成、存储与核验之证据,试拟三项推定规则:(1)若当事人提交的网络数据是由区块链平台自动生成的,

[78] 参见前引[60],刘品新文,第62页。

[79] Act relating to Miscellaneous Economic Development Provisions of Vermont, House Act 868, 2016.

[80] eIDAS Regulation.

得推定该数据属实，但存在足以反驳的相反证据时除外。^[81]（2）若当事人提交的网络数据在生成时已同步存入区块链平台的，或者在取证时或其后的合理时间内存入的，或者虽未在合理时间内入链但存在多次系列入链等足以综合认定等情形的，得推定该数据入链后未经改变，但存在足以反驳的相反证据时除外。^[82]（3）若网络数据的哈希值被存入区块链平台，且经核验一致的，得推定该数据自哈希值入链时起即未经改变，但存在足以反驳的相反证据时除外。^[83]

司法认知是一种同推定有近缘关系的认定方法，是法官在不需当事人举证的情况下对符合特定情形的案件事实予以确认。其中，除了“众所周知的事实”外，“既决事实”亦属司法认知的范畴。“民事诉讼证据规定”第10条将其具体化为“已为仲裁机构的生效裁决所确认的事实”“已为人民法院发生法律效力裁判所确认的基本事实”“已为有效公证文书所证明的事实”等。现阶段我国权力机关等公共部门较普遍地开展了区块链存储、核验工作，前述几项“事实”认知规则显然可以延展适用于区块链存储、核验之证据。考虑到少数部门已搭建了区块链生成平台以提高工作效率（如前文述及部分法院将智能合约技术方案用于司法执行智能化），前述几项“事实”认知规则亦可延展适用于区块链生成之证据。将上述认知规则延展适用于区块链证据，是基于以下几点理由。

一是基于法官依职权知悉的角度。在我国，有影响力的区块链存证平台主要由法院主导，法院负责对平台的设计、开发和运营，法官对事后开展数据查询和核验等事项亲历亲为。如此形成的区块链存储、核验之证据，显然属于法官审判上的“知悉”事项，应当对其予以司法认知。以广州互联网法院的电子证据平台“网通法链”为例，它形成了一个集数据生成、存证、取证、采信为一体的综合服务体系，其接入机构首先指向广州互联网法院、广州市中级人民法院、广州知识产权法院、广州铁路运输中级法院，这意味着四家法院对入链数据信息均有掌握。因此，这四家法院的法官可以通过查询“网通法链”对入链数据的真实性进行确认。

二是基于公证机构出具公证书的角度。在我国，许多区块链存证平台将公证机构作为节点，公证机构可以静默地参与区块链存证活动。数据入链时信息被同步共享给公证机构，一旦发生纠纷便可根据需要由公证机构出具公证书。实际上，接入“网通法链”的机构还包括广州市南方公证处、广州公证处这两家公证机构。从这个角度看，办案法院完全可以依据入链数据“经由公证”而直接确认其真实性。此即属“已为有效公证文书所证明的事实”，法官应予确认，这样就能加快区块链证据被广泛认可的速度。需要说明的是，这种新的公证方式意味着公证机构预先加入区块链节点，并对区块链证据的真实性进行背书。

三是基于其他节点单位作出生效裁断等处理的角度。例如，在“网通法链”中，接入的机构还包括广州仲裁委员会、广州市人民检察院、广州市司法局等多家单位。这意味着任何数据一旦存入“网通法链”平台，仲裁机构可以据此作出仲裁，检察机关、行政机关可以将其作为证据使用。联盟链中任一节点单位基于入链数据作出生效裁断等处理，即意味着对该入链

[81] 相反证据通常是“赖以产生数据的区块链平台是否可信”等。

[82] 相反证据通常是“多版本入链、选择性举证”等。“多版本入链、选择性举证”是指，当事人或其代理人就某一个事实相关的电子证据（如电子合同等）生成多个版本，分别传至区块链保存，在将来发生争议时择其有利者用作证据。

[83] 相反证据通常是“多版本入链、选择性核验”或“多版本保留”等。它指的是，当事人或其代理人就某一个事实相关的电子证据（如电子合同等）生成多个版本，对每个版本分别计算哈希值并分别传至区块链保存，在将来发生争议时择其有利者作为证据进行校验。参见陈平祥、姜琪、朱冠琳：《论运用区块链技术提取和审查刑事电子数据》，载周汉华主编：《网络信息法学研究》2019年第1期，中国社会科学出版社2019年版，第165页。

数据真实性的认可。

在各种有影响力的区块链存证平台中，法院、公证机构、仲裁机构、检察院、司法行政机关等主体处于“联盟”关系中，实现了一步存证、多元取证的效果。这使得我国着眼于司法认知的角度为区块链证据建立规则，不仅有量增的进步性，更有质变的进步性。以下亦针对各种区块链证据，试拟一项司法认知规则：当事人提交的网络数据是由区块链平台生成、存储或核验的，且系可由法庭在链上检索的，或者由作为区块链节点的公证机构、仲裁机构、检察机关、行政机关出具法律文书的，法庭应当确认该数据的真实性，但有相反证据足以推翻的除外。

如此一来，我国就可以形成“区块链+推定”“区块链+司法认知”并行的新型区块链证据真实性规则。这一规则体系能够很好地发挥区块链证据的优势，其既能适应司法系统直接参与区块链平台生成、存证、核验数据的情况，也能适应无需司法系统介入的各种社会性区块链平台的情况，更有利于今后更加开放地探索区块链跨域、跨链互认等新领域。

Abstract: Blockchain evidence refers to all evidentiary materials based on blockchain technology, which can be divided into blockchain-generated evidence, blockchain-stored evidence and blockchain-verified evidence. Based on this cutting-edge technology, blockchain evidence has unique values in clarifying the facts of complex cases, analyzing large amounts of heterogeneous digital evidence and promoting the development of intelligent judicial system. In adopting related legal rules, China should adopt a rational attitude towards the blockchain evidence, adhere to the principles of non-discriminatory treatment and deferential classification, and focus on the issue of authenticity. Technological characteristics such as hash verification, time locking and node verification have greatly enhanced the veracity of blockchain evidence, which can not only guarantee the verification of data after entering the chain, but also optimize the verification of the data before entering the chain. Based on the above two advantages and the existing authenticity rules of electronic evidence, China should review the legislative defects in the Rules of Online Litigation of People's Courts, explore and draw on comparative experiences, and make rules on the judicial cognition and presumption of the veracity of blockchain evidence.

Key Words: blockchain evidence, electronic evidence, rules of evidence
