法学研究 Chinese Journal of Law
Vol.44，No.2（2022）

电子数据的技术性鉴真

谢登科*

内容提要：电子数据鉴真是信息时代重要的证据问题。我国司法机关在实践中尝试将完整性校验、可信时间戳、数字签名、区块链存证等信息技术应用于电子数据鉴真。这既源于传统的“保管链证明”和“独特性确认”鉴真方法无法完全适应电子数据的虚拟性、可分离性、海量性等特征，也源于证据鉴真方法的开放性所提供的制度空间和在线诉讼推广适用所产生的内在需求。技术性鉴真并非简单地将信息技术应用于电子数据鉴真，其也会带来电子数据鉴真方法和规则的改变。技术性鉴真在价值功能、鉴真标准等方面与传统鉴真方法并无区别，但在内在机理、证明责任、程序保障等方面存在较大差异，因此有必要在整合现有制度的基础上构建电子数据技术性鉴真规则。技术性鉴真有其适用边界，其主要适用于电子数据“单独提取”模式，在“转化收集”模式中的适用具有限制性，在“一体收集”模式中的适用则具有阶段性；技术性鉴真方法可与传统鉴真方法交叉适用，但也存在独立适用的发展态势；技术性鉴真仅能解决电子数据的形式真实性问题，而无法保障其实质真实性。在电子数据技术性鉴真中，应保障诉讼主体的平等参与和有效对抗。

关键词：电子数据　鉴真　完整性校验　数字签名　区块链存证

一、问题的提出

随着信息技术和数字经济的不断发展，人们使用计算机、手机等电子设备实施各种行为会在网络空间或电子设备中留下“痕迹”，它们会以电子数据的形式存在。电子数据已经成为网络信息时代的“证据之王”，〔1〕电子数据鉴真也已成为网络信息时代重要的证据问题。科学技术是把“双刃剑”，既可以用它来修改、伪造电子数据从而提高鉴真成本和难度，也可以用它来创新电子数据鉴真方法。传统实物证据鉴真主要通过“保管链证明”和“独特性确认”

* 吉林大学法学院教授。
本文系国家社科基金重大项目“中国特色刑事证据理论体系研究”（18ZDA139）、国家社科基金一般项目“电子数据区块链存证研究”（21BFX014）的阶段性成果。

〔1〕 参见刘品新：《电子证据法》，中国人民大学出版社 2021 年版，第 3 页。

两种方法。[2] 而电子数据具有虚拟性、系统性等特征，这不仅决定了其证据形态、取证模式与传统实物证据存在较大差异，也决定了以人力识别和记录为基础的传统鉴真方法在用于电子数据时会存在较大局限。

实践中，电子数据鉴真除了采用传统的“保管链证明”和“独特性确认”方法外，我国司法机关也尝试采用完整性校验、可信时间戳、数字签名、区块链存证等信息技术，由此产生了电子数据的技术性鉴真，即借助信息技术实现对电子数据同一性和真实性的证明。科学技术在传统实物证据鉴真中也不罕见，比如通过声纹鉴定实现对声音同一性和真实性的证明，借助笔迹鉴定实现对笔迹同一性和真实性的认定。但是，传统实物证据鉴真中对科学技术和专业知识的使用，主要是为了提升人工识别能力，这是建立在人工感知与识别的基础上的。而电子数据作为信息技术的产物，一方面，在电子数据鉴真中，技术方法的使用具有常态性；另一方面，在电子数据技术性鉴真中，存在摆脱依靠人工记录识别而转向算法程序自动比对的发展态势，由此会带来规范效力、运行程序等方面的制度变化。

可以说，各种新兴信息技术的诞生，不仅衍生出新型电子数据，也扩展了电子数据的鉴真方法。比如，区块链技术既催生了区块链电子数据，也带来电子数据的新型鉴真方法——区块链存证。北京、杭州、广州互联网法院分别组建了“天平链”“司法链”“网通法链”等存证平台，截至 2019 年 12 月底，这三个区块链平台存证的电子数据已近 20 亿条。[3] 当然，电子数据技术性鉴真并非我国独有，美国的司法实践中也将数字签名、完整性校验等技术方法用作电子数据的鉴真方法。[4] 比如，美国《佛蒙特州证据规则》第 902 条第 13 项明确将区块链存证作为电子数据自我鉴真方法之一。[5] 通过区块链存证等信息技术实现电子数据鉴真，已成为国际上共同的发展趋势。

在规则制定层面，最高人民法院、最高人民检察院、公安部 2016 年联合发布《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》（以下称“电子数据规定”），将完整性校验作为电子数据的鉴真方法之一。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》（以下称“互联网法院审理案件规定”），将可信时间戳、数字签名、哈希值校验、区块链存证等技术手段，作为互联网法院审理案件中电子数据鉴真的重要方法。2021 年最高人民检察院《人民检察院办理网络犯罪案件规定》，将完整性校验、数字签名、数字证书作为电子数据鉴真的重要方法。2021 年最高人民法院《人民法院在线诉讼规则》（以下称“在线诉讼规则”），将区块链存证作为在线诉讼中电子数据的鉴真方法，规定了其规范效力、审查方法等内容。

在理论研究层面，理论界对电子数据鉴真问题的探讨，仍主要围绕传统鉴真方法，对技术性鉴真方法关注不足。[6] 这既无法与技术性鉴真方法的重要性相适应，也无法为现有信息技术和未来新兴技术应用于电子数据鉴真提供理论支撑。我国电子数据技术性鉴真的实践探索已

〔2〕 参见陈瑞华：《实物证据的鉴真问题》，《法学研究》2011 年第 5 期，第 131 页以下。

〔3〕 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 150 页。

〔4〕 See Paul R. Rice, *Electronic Evidence: Law and Practice*, American Bar Association Press, 2005, pp. 249 – 256.

〔5〕 See Vermont Rules of Evidence 902 (13).

〔6〕 例如刘品新：《电子证据的鉴真问题：基于快播案的反思》，《中外法学》2017 年第 1 期；谢登科：《电子数据的鉴真问题》，《国家检察官学院学报》2017 年第 5 期；刘译矾：《论电子数据的双重鉴真》，《当代法学》2018 年第 3 期；郭金霞：《电子数据鉴真规则解构》，《政法论坛》2019 年第 3 期。

处于世界前列，但理论层面缺乏系统、深入研究，对其法律或规范性质、运行程序、审查方法等缺乏清晰认识，导致实践探索和规则创制遭遇各种困境。比如，我国现有规则虽然确立了区块链存证电子数据具有“推定真实”的效果，但缺乏对其法律或规范性质的理论分析，也未将其纳入现有证据规则特别是鉴真规则进行探讨，这就可能导致实务界对其“真实性”效力期待过高。〔7〕

信息技术在电子数据鉴真中的应用，可在不同程度上化解传统鉴真方法适用于电子数据时的局限性，同时也会引起电子数据鉴真方法和规则的改变。技术性鉴真方法的价值功能、鉴真标准与传统鉴真方法并无区别，但其在内在机理、证明责任、程序保障等方面存在差异。因此，本文拟对电子数据的技术性鉴真予以理论分析，考察技术性鉴真兴起的原因及常见类型，通过与传统鉴真方法的比较来厘清技术性鉴真方法的特点，并在此基础上提出电子数据技术性鉴真规则的主要内容和方法适用边界。

二、电子数据技术性鉴真兴起的原因

其一，电子数据属于实物证据，对其自然可以采用物证、书证等传统实物证据的鉴真方法，在现有规定和实践运行中，“保管链证明”和“独特性确认”仍然是电子数据鉴真的重要方法，比如在电子数据的收集中需制作取证笔录、同步录像、见证人见证等。但是，电子数据与传统实物证据在存在形态、取证模式等方面有较大差异，传统鉴真方法可能存在适用上的局限性。比如，作为传统鉴真方法的“保管链证明”和“独特性确认”是以物证、书证为基础的，相比于传统实物证据，电子数据具有虚拟性、可分离性、海量性等特征，这就决定了仅采用传统鉴真方法可能无法实现有效鉴真。

首先，电子数据的虚拟性决定了，仅使用证人证言、取证笔录等方法，将难以保障电子数据信息的同一性和真实性。传统实物证据是以其物质属性、外部特征等信息来发挥证明作用的，这些信息可以通过人的直接感知、笔录记载等予以固定。而对于电子数据，人们无法通过直接感知予以识别，须借助相应电子设备展示才能感知或识别。对于电子数据所处的虚拟空间，办案人也不能直接进入，而需要借助相关软硬件设备才能感知、收集涉案电子数据。在不借助相关技术手段的情况下，人们只能感知通过电子设备展示的图文信息及电子设备本身。从鉴真方法看，对于具有物质形态的存储介质，可以适用“保管链证明”和“独特性确认”鉴真方法；而电子数据的虚拟性、无形性等特点，则可能导致传统鉴真方法在电子数据鉴真中无法独立适用。比如，对于通过“微信生成器”变造、篡改或伪造的微信聊天记录类电子数据，若不借助相应技术方法，仅靠肉眼识别，则很难发现其是否存在增减或修改。

其次，电子数据的可分离性决定了，通过对存储介质的鉴真，一般难以有效实现对电子数据自身的鉴真。传统实物证据所承载的证据信息通常依附于证据的物质形态而存在，若物质形态没有变化，其承载的证据信息通常也不会发生变化。这就决定了，若能保障实物证据的同一性，就可以保障其承载的证据信息的同一性。但是，电子数据所承载的证据信息并不依附于其存储介质，且电子数据与其存储介质之间具有独立性和可分离性。〔8〕此种特征决定了仅依靠

〔7〕 参见刘品新：《论区块链证据》，《法学研究》2021 年第 6 期，第 138 页。

〔8〕 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 125 页。

对存储介质的鉴真，并不足以实现对电子数据自身的鉴真。在存储介质没有发生变化的情况下，仍然有可能无法保障电子数据的同一性和真实性。比如，在没有物理接触或操控存储介质的情况下，可以通过无线传输等方法修改电子数据。电子数据的可分离性特征也使得取证中可以仅收集与案件有关的电子数据，而不收集其原始存储介质。因此，在“去原始存储介质”的电子数据取证方式下，就无法完全通过存储介质鉴真来实现电子数据鉴真。

最后，电子数据的海量性特征决定了，传统鉴真方法无法胜任对电子数据同一性的比对和确认。传统实物证据的数量相对有限，通过取证笔录记载的证据信息和过程信息、见证人所要感知和记忆的信息也都相对有限。但是，电子数据具有海量性特征，占据相同物理空间的存储介质比如 U 盘、硬盘等，可以存储海量数据，其存储的证据信息可能是相同体积下传统实物证据的很多倍。比如，在“快播案”中，有关部门执法检查扣押了四台涉案服务器，每台容量 10TB。〔9〕对于海量的电子数据，若不借助现代信息技术，仅依靠传统的证人证言、取证笔录等方法，既无法实现对电子数据的完整记录和识别，也会极大增加鉴真成本和难度。

信息技术可在不同方面克服电子数据自身特征所带来的鉴真难题。电子数据属于科学证据，科学证据的发现、收集、保全等需要借助现代科学技术。〔10〕互联网、人工智能、区块链等信息技术在司法活动中的推广应用，也引发了电子数据真实性保障和防篡改机制的变革。在电子数据取证中，可以采用区块链存证等技术来保障电子数据的完整性和真实性。信息技术应用于电子数据鉴真，能有效适应电子数据自身的特点：（1）技术性鉴真能有效适应电子数据的虚拟性特征。电子数据技术性鉴真方法实际上属于算法程序，其运行过程就是数据处理过程，并不直接以实物形态的物品为处理对象。（2）技术性鉴真可以保障收集提取电子数据的完整性。在电子数据取证中，可以通过镜像复制实现收集电子数据的完整性，并在收集复制电子数据后计算电子数据的完整性校验值。然后，可以通过完整性校验值比对来保障复制提取的电子数据具有一致性和完整性。（3）技术性鉴真方法可高效适用于海量电子数据。比如，通过 MD5（Message Digest Algorithm 5）算法进行完整性校验，无论多大存储量的数据，经过运算后都会得到 128 位散列值；对于容量不超过 4GB 的电子数据，可在数据上传完毕后几秒至几分钟内完成可信时间戳认证。

其二，鉴真方法的开放性为引入电子数据技术性鉴真方法提供了制度空间。鉴真本质上是对实物证据同一性、真实性的证明。此种证明属于对证据种类、调查程序、证明标准的法律要求相对宽松的自由证明，〔11〕因此鉴真方法可以保持适当的开放性和灵活性。比如美国《联邦证据规则》第 901 条 b 款列举了十种鉴真方法，此种列举仅意在满足鉴真要求的证据类型，而不具有排他性。〔12〕为应对电子数据提出的各种挑战，有美国学者曾建议制定新规则专门调整电子数据鉴真问题，但美国证据咨询委员认为制定新规则并非最佳方案，于是仅在 2017 年修订后的《联邦证据规则》第 902 条中增加了电子数据自我鉴真的两种新方法，因为现有鉴真规则具有足够的灵活性和宽泛性，可以涵盖电子数据鉴真问题。〔13〕我国“电子数据规定”

〔9〕 参见北京市海淀区人民法院（2015）海刑初字第 512 号刑事判决书。

〔10〕 参见陈学权：《科技证据论——以刑事诉讼为视角》，中国政法大学出版社 2007 年版，第 52 页。

〔11〕 参见闵春雷：《严格证明与自由证明新探》，《中外法学》2010 年第 5 期，第 184 页。

〔12〕 参见［美］阿维娃·奥伦斯坦：《证据法要义》，汪诸豪、黄燕妮译，中国政法大学出版社 2018 年版，第 226 页。

〔13〕 See Paul W. Grimm, Daniel J. Capra & Gregory P. Joseph, *Authenticating Digital Evidence*, 69 Baylor Law Review 3 – 4 (2017).

第 5 条、第 23 条采取“列举 + 兜底”的方式，规定了保障电子数据完整性的各种方法。此种规定方式符合鉴真方法开放、灵活的要求，为在电子数据鉴真中引入技术性鉴真方法提供了制度空间。任何用来证明电子数据完整性和真实性的材料或方法，都可以在电子数据鉴真中使用，其中就包括信息技术方法。

其三，在线诉讼促进了电子数据技术性鉴真的推广适用和独立发展。在线下诉讼中，电子数据取证大多采取“转化收集”模式，庭审中主要是出示电子数据的截图、照片、打印件。〔14〕“转化收集”模式虽然在线下诉讼中简便易行，但并不利于电子数据技术性鉴真的推广适用。随着信息技术的迅速发展，在线诉讼已成为当下重要的纠纷解决和审判方式之一。在线诉讼中会面临大量电子证据审查认定问题，这里的“电子证据”不仅包括电子数据，也包括经过电子化处理的物证、书证等传统实物证据，涉案电子数据的生成、存储、移送等环节也都通过网络方式在线完成，这会使得传统鉴真方法适用于在线诉讼的局限性更为突出。对此，需要在传统的“保管链证明”和“独特性辨认”鉴真方法之外，探索适用于在线诉讼的电子数据鉴真方法，采用区块链存证等技术手段审查认定电子数据真实性将成为在线诉讼中的常态。

三、电子数据技术性鉴真方法的常见类型

完整性校验、可信时间戳、数字签名、区块链存证是我国司法实践中较为常见的电子数据技术性鉴真方法，“电子数据规定”“互联网法院审理案件规定”“在线诉讼规则”等规范性文件，已经对这些方法作了规定。

（一）完整性校验

完整性校验值，是使用散列函数等特定算法，对电子数据进行计算而得出的用于校验电子数据完整性的数值。电子数据的完整性是电子数据真实性的前提和基础，若缺乏完整性则意味着电子数据可能存在增减、破坏或丢失等情况，其真实性可能无法得到保障。〔15〕在电子数据收集提取和审查认定中，通常使用完整性校验来保障电子数据的完整性，哈希值计算比对是最主要的完整性校验方法。哈希值是将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，其主要有以下特征：（1）唯一性。两个不同数据经过哈希函数运算后得到的哈希值不同。（2）确定性。对同一数据输入或相同数据输入，无论经过多少次哈希函数运算，得到的哈希值都相同。（3）不可逆性。在仅有哈希值的情况下，无法逆向还原出哈希值所对应的原始输入数据。〔16〕基于这些特征，任何一条电子数据，比如文本文件、应用程序、音视频文件等，不管其存储量多大，有且仅有唯一的哈希值。若电子数据发生增减或修改，其哈希值也会发生变化。较为常见的哈希值算法包括 MD5、SHA（Secure Hash Algorithm），由于 SHA 算法的强度和安全性更高，其已成为目前主流的完整性校验方法。〔17〕

完整性校验是电子数据鉴真的重要方法，在电子数据取证中，是否计算完整性校验值，有

〔14〕 参见胡铭：《电子数据在刑事证据体系中的定位与审查判断规则——基于网络假货犯罪案件裁判文书的分析》，《法学研究》2019 年第 2 期，第 175 页。

〔15〕 参见喻海松：《刑事电子数据的规制路径与重点问题》，《环球法律评论》2019 年第 1 期，第 38 页。

〔16〕 参见陈鹏：《区块链本质》，清华大学出版社 2019 年版，第 48 页。

〔17〕 参见刘浩阳等：《公安机关办理刑事案件电子数据取证规则释义与实务指南》，中国人民公安大学出版社 2020 年版，第 22 页。

时甚至直接影响能否对电子数据进行有效鉴真。例如，在陈某贩卖毒品案中，公安机关从被告人处扣押手机后提取涉案电子数据，制作了勘验检查笔录，但该笔录没有持有人、见证人签章，也没有记载提取过程和内容，取证过程没有录像，也没有计算电子数据完整性校验值。法院认为该电子数据取证程序存在重大瑕疵，且不能作出合理解释，故对该电子数据予以排除。〔18〕再如，在占某、詹某等非法控制计算机信息系统案中，占某辩护人提出，电子数据勘验检查笔录没有见证人签名且电子数据取证过程未全程录像，电子数据的真实性存疑。法院经审理后认为：因该案涉及异地办案，侦查人员众多，电子数据取证过程虽无见证人签名和全程录像，但已以截图形式保存，能客观反映勘验提取电子数据的真实性，被告人詹某也认可软件源代码存储在相关存储介质中的事实；并且涉案电子数据均有完整性校验值，内容比对一致，电子数据具有完整性，故该电子数据可以作为定案依据。〔19〕

上述两个案例中，涉案电子数据因是否计算了完整性校验值而得到了不同的认定结果。在陈某贩卖毒品案中，侦查机关扣押手机后没有作封存处理，没有制作同步录像，取证笔录欠缺签章、要素不全，法院无法借助“证据保管链”方法对电子数据进行鉴真。该案取证中也没有计算电子数据完整性校验值，不能排除电子数据被增减、篡改的可能性。控方无法有效证明电子数据的真实性，无法对电子数据作有效鉴真，故法院对该电子数据予以排除。在占某、詹某等非法控制计算机信息系统案中，电子数据取证也欠缺见证人见证、同步录像，法院无法借助“证据保管链”方法进行鉴真。法院虽然主张依据“截图保存”“被告人认可”“完整性校验”来认定电子数据的真实性，但电子数据鉴真实际上主要依据完整性校验。这是因为“截图”的真实性有待审查确认，存储于相关存储介质的电子数据在被收集提取后是否存在增减、修改的情况也无法确认，而侦查机关提取电子数据后计算得出的完整性校验值具有确定性和唯一性，后经比对发现完整性校验值未发生变化，故法院确认了该电子数据的真实性。

对于电子数据技术性鉴真规则，“电子数据规定”和 2019 年公安部《公安机关办理刑事案件电子数据取证规则》（以下称“电子数据取证规则”）等规范性文件建立了以完整性校验为核心的体系。其一，通过网络在线提取、冻结、调取、检查等方式收集电子数据时，侦查机关应计算电子数据的完整性校验值。其二，侦查机关在电子数据的收集取证中，需制作相关取证笔录，在取证笔录中应注明完整性校验值的类型、具体数值。其三，证据保管部门在接收电子数据时应审查比对其完整性校验值，将比对情况和结果记载于接收笔录中。其四，电子数据在保管、移送、检验等环节若发生修改，会导致其完整性校验值不一致，若完整性校验值经比对确认一致，则可初步认定电子数据的真实性。在美国的司法实践中，计算、比对完整性校验值也是实现《联邦证据规则》第 902 条第 14 项中电子数据自我鉴真的常见方法。〔20〕

（二）可信时间戳

可信时间戳是由时间戳服务中心（Time-Stamp Authority，TSA）签发的电子凭证，可用于证明电子数据自申请可信时间戳之后的完整性和未被篡改性。在时间戳认证中，申请人需将收集的电子数据上传至时间戳服务中心，时间戳服务中心收到电子数据后对其进行哈希值运算，并对该哈希值和收到电子数据的时间进行数字签名，生成可信时间戳认证书发送给申请人。可

〔18〕 参见云南省通海县人民法院（2018）云 0423 刑初 279 号刑事判决书。

〔19〕 参见浙江省嘉善县人民法院（2019）浙 0421 刑初 257 号刑事判决书。

〔20〕 See Andrew Schupanitz & Jacklin Chou Lem, *Judges' Treatment of Federal Rules of Evidence 902 (13) and 902 (14)*, 68 DOJ Journal of Federal Law and Practice 112 (2020).

信时间戳生成后，便锁定了电子数据在哈希值生成时的状态。在此之后，电子数据是否保持了完整性，可借助时间戳服务中心的逆向解码来验证。法院在通过可信时间戳审查电子数据的真实性时，需向时间戳服务中心上传电子数据及其对应的可信时间戳认证书。若验证显示未被篡改，且时间码与申请可信时间戳的时间一致，则表明该电子数据未被篡改，可以确认其完整性和真实性。

可信时间戳也是常见的电子数据技术性鉴真方法，但其在刑事司法中相对较少适用，而广泛应用于民事诉讼、商事仲裁等领域。这可能源于刑事司法对证据合法性的要求较高，其中就包括对取证主体合法性的要求，取证主体不合法会影响证据的证据能力。〔21〕若公安机关、检察机关等国家专门机关委托取证公司负责收集电子数据并制作可信时间戳，则可能因为取证主体合法性不足而减损电子数据的证据能力，这就使得司法机关不愿在刑事案件中使用可信时间戳来进行电子数据鉴真。另外，刑事诉讼领域中电子数据的鉴真方法较为多元，既可以采用取证笔录、同步录像、见证人见证等方法，也可以采用完整性校验的技术性方法。而在民事诉讼中，需要当事人或其诉讼代理人自行收集、提交有关证据。当事人可能因为欠缺法律知识而未在证据收集保管环节制作取证笔录；代理律师即便在取证中制作了取证笔录，但相比公安机关、检察机关等国家专门机关，法院可能会因为私人主体制作的取证笔录可信性较差，而排斥将其取证笔录作为实物证据鉴真的依据。因此，民事司法中电子数据的鉴真方法相对单一，主要通过公证、鉴定等方式，其运行成本相对较高。以可信时间戳等技术方法替代公证，则可降低电子数据鉴真成本，减少当事人的诉讼支出。“互联网法院审理案件规定”第 11 条第 2 款将可信时间戳、数字签名、区块链存证等规定为电子数据的技术性鉴真方法，就主要缘于民事诉讼中对电子数据真实性的审查主要依靠公证，以及在线诉讼会涉及大量电子数据，需要打破通过公证认定电子数据真实性的单一途径，以技术手段和配套制度来保障电子数据的真实性。〔22〕除了互联网法院审理的民事案件，其他法院在审理知识产权、网络购物、网络信贷等民事案件时，也大量使用可信时间戳进行电子数据鉴真。例如，在汉华易美公司与麦科田公司侵害信息网络传播权纠纷案中，原告向法院提交了时间戳认证的涉案微信图片。法院经审理后认为：可信时间戳认证书由我国法定时间戳机构授时，并由第三方时间戳服务机构颁发，能确定“什么人在什么时候拥有什么样的电子数据”的客观事实，是不能篡改和伪造的；原告对涉案图片取证是在登录时间戳中心网页后，再登入被告微信公众号进行证据保全，取证过程及内容均由时间戳中心予以认证，故对该电子数据的真实性予以确认。〔23〕

（三）数字签名

数字签名也称电子签名，它是在数据电文中以电子形式所含或所附用于识别签名人身份并表明签名人认可其中内容的数据。数字签名采取非对称加密技术，发送者运用非对称加密技术生成公钥和私钥，对发送数据信息进行数字签名，然后将公钥和签名数据信息发送至接受方，接受方可以使用验证算法来核实该数据信息是否由发送者签名。非对称加密技术可以保障数据

〔21〕 参见张建伟：《证据法要义》，北京大学出版社 2014 年版，第 138 页；陈瑞华：《刑事证据法学》，北京大学出版社 2018 年版，第 137 页。

〔22〕 参见胡仕浩、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。

〔23〕 参见天津市第三中级人民法院（2019）津 03 知民初 1193 号民事判决书。

信息的完整性、可靠性和身份可认证性。〔24〕在交易内容真实性、信息身份关联性等发生争议时，数字签名就成为此类电子数据的重要鉴真方法。

数字签名是对交易类电子数据进行鉴真的重要方法，其在民事诉讼领域较多适用。“电子数据取证规则”第 24 条规定，在网络在线提取电子数据中，必要时可以收集数字签名、数字证书等关联性信息。这主要是考虑到：网络在线提取的对象是电子数据，而不是其原始存储介质，原则上应通过计算完整性校验值来保障电子数据的完整性，但为了防止网络因素导致完整性校验值发生变化，故将数字认证、数字签名等也纳入收集范围，以确保电子数据不被篡改。〔25〕例如，在雷某与聂某民间借贷纠纷案中，法院认为：雷某虽向法院提交了借贷宝 APP 的借款操作流程、用户注册信息、借出协议、转账记录等电子数据，但借出协议并无双方电子签名，无法证实出借人、借款人身份是否真实，故驳回原告的诉讼请求。〔26〕再如，在王某与杨某民间借贷纠纷案中，王某向法院提供了其与证人高某微信账号 W 的聊天记录；高某确认微信账号 W 系其本人账号，但否认此聊天信息系其本人发出，不认可聊天记录的真实性，并提出可能是王某盗用了微信账号或使用“微信生成器”类软件生成聊天记录。鉴定意见认为，该微信聊天记录截图不符合常见“微信生成器”所生成图片的特征，该截图未见剪辑修改痕迹。杨某认为该鉴定意见仅能证明微信聊天记录未造假，但不能证明相关聊天信息系高某所发。法院经审理后认为：高某作为微信账号 W 的电子签名人，该账号对外发出电子数据应视为高某的行为及意思表示；若高某发现其微信账号无法正常登录使用，应意识到可能被他人盗号并应积极采取措施预防可能发生的风险，但高某作为电子签名人未提供证据证明其账号被王某盗用，故对该电子数据予以采信。〔27〕

上述是民事司法领域将数字签名用作电子数据鉴真方法的案例。在雷某与聂某民间借贷纠纷案中，电子借款协议没有当事人的数字签名，在无法对该电子数据进行鉴真的情况下，法院驳回了原告的诉讼请求。在王某与杨某民间借贷纠纷案中，对微信聊天记录截图的鉴真涉及两方面内容：该截图是否系伪造；聊天信息是否系证人高某所发。前者主要经由鉴定意见认定没有伪造、篡改痕迹而予以鉴真，可实现对电子数据形式真实性的认定；后者主要涉及身份关联真实性的鉴真问题，即聊天信息是否系证人高某所发。法院将数字签名作为该电子数据身份关联性的重要鉴真方法，即高某作为微信账号 W 的数字签名人，可以推定该账号聊天信息为其本人所发。这里的“推定真实”就源于微信账号中的数字签名可以实现对身份关联性的初步证明。其一，数字签名本身蕴含了签名人的身份信息，有助于确保签名就是文件创始人所签，也有助于防止他人伪装成特定文件创始人，从而为身份关联性提供初步的筛查或证明机制。其二，通过数字签名发送的数据信息，需要经过公钥进行加密处理，从而生成该传递信息所对应的哈希值，而哈希值的确定性和唯一性保障了发送数据信息的完整性和真实性。其三，数字签名解决了数据电文的身份识别和确认问题，而公正、权威的第三方机构对签名人身份信息、相关资料的核实管理，〔28〕可以增强对电子交易主体和内容的信任程度，增强电子签名的真实性与可靠性。

〔24〕 参见王学光：《电子证据法律问题研究》，法律出版社 2019 年版，第 37 页。
〔25〕 参见前引〔17〕，刘浩阳等书，第 126 页。
〔26〕 参见四川省广安市中级人民法院（2020）川 16 民终 1027 号民事判决书。
〔27〕 参见北京市门头沟区人民法院（2014）门民（商）初字第 4239 号民事判决书。
〔28〕 参见电子签名法第 20 条至第 22 条的规定。

（四）区块链存证

区块链采取的分布式记账技术，可实现对存证数据的分布式存储，让存证数据具有较强的防篡改性。数据被上传至区块链之后，在没有修改后续区块的情况下，不能通过单独改变某个节点来修改数据。〔29〕可以说，区块链存证综合了分布式存储、完整性校验、可信时间戳等多项信息技术，能够为电子数据的真实性提供技术保障。

区块链作为当下网络信息技术的新兴产物，能有效保障所存储信息的安全性和可靠性，这使其成为电子数据的技术性鉴真方法之一。当前，我国司法机关正在开展电子数据区块链存证的实践探索，区块链存证的司法适用越来越普遍。例如，在中文在线公司与京东公司作品信息网络传播权纠纷案中，中文在线公司使用 IP360 平台对涉案 APP 录屏取证，收集的电子数据被同步上传至司法联盟链存证；京东公司对该电子数据的真实性提出异议。法院经审理后认为：中文在线公司提交的电子数据经区块链存证，其完整性较为可靠，在无相反证据的情况下，其真实性应予确认，可以作为认定事实的初步证据；京东公司虽对电子数据的真实性提出异议，但其并未提交证据证明存证过程存在技术缺陷或其他影响证明效力的情况，故对该主张不予支持。〔30〕再如，2017 年 1 月至 2019 年 3 月，王某通过网络实施诈骗他人财物行为 176 起。由于本案被害人众多且分散于全国各地，司法机关采用区块链技术对数据进行存证，法院经审理后将区块链存证的电子数据作为定案依据。〔31〕

上述是民事、刑事司法领域将区块链存证用作电子数据鉴真方法的案例。在中文在线公司与京东公司作品信息网络传播权纠纷案中，法院明确了区块链存证的规范效力：（1）真实性推定效力。法院认为经区块链存证的电子数据，其完整性较为可靠，具有可反驳的推定真实性效力。基于此种效力，法院将电子数据真实性的证明责任配置给京东公司，京东公司未提供证据证明电子数据不真实，应承担证明不能的法律后果，故法院对其主张不予支持。（2）初步证据的效力。法院认为区块链存证电子数据可以作为证明案件事实的“初步证据”，这意味着该电子数据的证据能力已经得到确认，但其证明力层面的真实性，即该电子数据所承载的内容信息的真实性，则仍需综合考虑其他证据及事实进行认定。

“互联网法院审理案件规定”第 11 条第 2 款采取“列举 + 概括”的方式，将前述四种方法并列为电子数据的技术性鉴真方法，而该款中的“等”是列举未尽之义，包括了用于电子数据收集、固定和防篡改的其他技术手段。从证据鉴真的角度看，完整性校验、可信时间戳、数字签名、区块链存证都可以用于保障电子数据的同一性和形式真实性。从信息技术的发展历程看，完整性校验是电子数据技术性鉴真方法的基础，其他技术性鉴真方法中都不同程度地包含了完整性校验。比如，数字签名需要通过哈希函数算法对数据形成加密摘要，区块链存证也需要借助哈希函数算法对存证电子数据形成摘要并将其存储于各个节点。数字签名、可信时间戳、区块链存证分别融合了身份确认、时间确认、分布式存储等技术，其保障电子数据真实性、防篡改性的效果更佳。但三者因其不同技术结构和特征，在电子数据鉴真中也各有侧重。比如，数字签名能实现对签名人的身份关联与确认，表明签名人对所签名之内容数据的认可，其在合同类电子数据鉴真中应用较多；可信时间戳可以为数据生成、提存时间提供证明，在知

〔29〕 参见前引〔16〕，陈鹏书，第 2 页。

〔30〕 参见北京市东城区人民法院（2018）京 0101 民初 4624 号民事判决书；北京知识产权法院（2018）京 73 民终 2163 号民事判决书。

〔31〕 参见余建华：《全国首例区块链存证刑事案宣判》，《人民法院报》2019 年 11 月 1 日第 3 版。

识产权案件中被广泛应用；区块链存证不仅融合了完整性校验、时间戳、数字签名等技术，其分布式账本技术也具有较强的防篡改功能。另外，数字签名、可信时间戳等技术中的第三方认证是建立在中心化信任机制上的，通过专业、权威的第三方认证来担保数据的真实性和可靠性。而区块链存证中的分布式账本技术则属于去中心化的信任机制，它通过对数据的多节点链式存储来防止数据被篡改。

四、技术性鉴真方法与传统鉴真方法的比较分析

电子数据鉴真需遵循实物证据鉴真规则，但其鉴真对象和鉴真方法与传统实物证据存在差异。从鉴真对象看，电子数据鉴真是要实现对电子数据信息自身的鉴真，而不是对电子数据信息载体或存储介质的鉴真。由于电子数据具有可分离性，电子数据取证并非必然采取“存储介质 + 电子数据”的封存、提取方式，而是可以单独收集、提取、复制电子数据，比如互联网法院在线诉讼中通常由作为第三方主体的网络平台经营者、网络服务提供商等将涉案数据直接导入电子诉讼平台。〔32〕从鉴真方法看，电子数据鉴真既可以使用传统鉴真方法，也有其自身特有的鉴真方法，这其中就包括完整性校验、可信时间戳、数字签名、区块链存证等技术性方法。为了厘清电子数据技术性鉴真的定位与特征，有必要将其与传统鉴真方法进行比较分析。

（一）相互关系

在电子数据鉴真中，对于技术性方法与传统方法的相互关系，有“嵌入说”“并列说”“替代说”等观点。“嵌入说”认为，技术性鉴真方法不具有独立性，这些方法仅是“证据保管链”“独特性确认”鉴真方法的内在要素，比如郭金霞就将数字签名视为“独特性确认”方式之一，将完整性校验视为“保管链证明”方式之一。〔33〕该观点可以解释完整性校验在刑事案件电子数据鉴真中的现实状况，因为完整性校验通常被嵌入各种笔录证据之中以对电子数据进行鉴真。但是，该观点无法为可信时间戳、区块链存证等技术手段独立应用于电子数据鉴真提供理论支撑。“并列说”和“替代说”都将区块链存证等技术手段视为独立的鉴真方法，这些观点对“互联网法院审理案件规定”“在线诉讼规则”中电子数据技术性鉴真的现有规定具有指导价值，但对刑事案件中完整性校验的嵌入式使用不能提供有效解释。“并列说”认为技术性鉴真方法与“证据保管链”“独特性确认”系并列关系，各自适用于不同情形下的电子数据鉴真。〔34〕“替代说”将技术性鉴真方法视为对传统鉴真方法的替代或部分替代，可用来弥补传统方法的不足。比如有司法实务人士就认为，在电子数据鉴真中引入数字签名、可信时间戳、区块链等技术手段，主要是弥补仅依公证程序认定电子证据真实性的不足。〔35〕此观点较为契合可信时间戳、区块链存证等技术手段独立适用于在线诉讼中电子数据鉴真的发展趋势，但忽视了传统鉴真方法在电子数据鉴真中仍有较大适用空间。

上述观点各有其合理性，但均未反映技术性鉴真方法与传统鉴真方法之相互关系的全貌。电子数据技术性鉴真方法与传统鉴真方法之间的关系，比较类似于电子数据与传统实物证据之间的关系。在电子数据发展的早期，由于法律尚未明确电子数据的证据地位，理论界和实务界

〔32〕 参见“互联网法院审理案件规定”第 5 条第 2 款的规定。
〔33〕 参见前引〔6〕，郭金霞文，第 62 页，第 65 页。
〔34〕 参见前引〔6〕，刘译矾文，第 93 页以下。
〔35〕 参见前引〔22〕，胡仕浩等文，第 24 页以下。

主要将其看作视听资料、书证、物证，仅有少数观点将其视为独立证据种类。〔36〕而在电子数据成为法定证据种类之后，其也无法游离于传统证据规则之外，仍然要受到传统证据规则的调整和规范，但这并不影响电子数据在存在形态、表现形式等方面所具有的独特性，其收集提取、审查认定规则也因此而具有自身的独特性。电子数据技术性鉴真方法的发展亦与此类似。最初的技术性鉴真方法，比如完整性校验，主要是嵌入传统鉴真方法进行适用。随着信息技术的不断发展，特别是可信时间戳、区块链存证等技术在电子数据鉴真中的推广适用，技术性鉴真方法逐渐摆脱了嵌入式适用而呈现出独立适用的发展态势。现有规则也赋予了技术性方法在电子数据鉴真中的独立地位，这体现在“互联网法院审理案件规定”“在线诉讼规则”对区块链存证等技术性鉴真方法的规定中。当然，技术性鉴真方法的独立适用并不意味着排斥传统鉴真方法，“证据保管链”“独特性确认”在电子数据鉴真中仍有较大适用空间。

从二者趋同的方面看，技术性鉴真方法在价值功能、鉴真标准等方面与传统的“证据保管链”“独特性确认”鉴真方法并无差异。首先，技术性鉴真方法和传统鉴真方法都是法院用来审查电子数据同一性和真实性的方法，是为采纳、使用该电子数据奠定基础。其次，鉴真是对实物证据或电子数据同一性和真实性的证明，这就涉及鉴真标准的问题。我国现有规则主要是在证据属性中的真实性层面关注实物证据鉴真，强调笔录类证据对实物证据来源和真实性的有效印证，〔37〕而缺乏对鉴真标准的设置和规定。在美国证据法理论和实务中，对实物证据鉴真并未设置很高的标准，只需达到《联邦证据规则》第 901 条 a 款规定的“足以支持证明某项事实为真”标准，其通常要求达到优势证据标准即可。此种鉴真标准并不会因为采用外部鉴真方法或自我鉴真方法而发生变化，〔38〕即采用技术性鉴真方法并不能降低或提高鉴真标准。

（二）独特之处

从二者趋异的方面看，技术性鉴真方法在内在机理、运行程序、证明责任等方面与传统鉴真方法存在差异，这为技术性鉴真方法的独立适用和规范地位奠定了基础。

其一，信息技术在电子数据鉴真中的应用，会引起鉴真方法内在机理的变化。对于传统实物证据，主要有“独特性确认”和“保管链证明”两种鉴真方法。前者需借助知情人员观察、感知实物证据的独有特征，通过在法庭上辨别、确认实物证据来证明其同一性和真实性；后者需要相关人员记录证据状态、流转保管等情况，并出庭就出示证据与案发时证据是否具有同一性作证。〔39〕对证据保管链的记录和证明，也需要借助经手人对证据的直接感知，记录证据名称、数量、特征等信息；法庭调查中需要他们对其经手的证据状况进行陈述。因此，传统鉴真方法是建立在人对证据状况、形态等信息之感知的基础上的。

电子数据的技术性鉴真则主要借助算法程序、数据代码等技术方法。比如，完整性校验主要通过哈希值实现电子数据的特定化和同一性比对，区块链存证主要借助分布式存储、非对称加密等手段防止电子数据被篡改。虽然运用技术方法对电子数据进行鉴真也需要借助人的审查和比对，但其并不以人对电子数据形态、特征等信息的感知为基础，而是将算法程序的运算结果作为比对依据。

〔36〕 参见前引〔1〕，刘品新书，第 22 页以下。

〔37〕 参见前引〔2〕，陈瑞华文，第 139 页。

〔38〕 参见前引〔13〕，Grimm 等文，第 8 页。

〔39〕 参见陈永生：《证据保管链制度研究》，《法学研究》2014 年第 5 期，第 176 页。

随着人工智能、算法取证等信息技术在电子数据取证中的推广适用，电子数据收集呈现出智能化、去人力化的发展趋势。人工智能取证、算法取证可以自动对收集到的电子数据进行完整性校验、区块链存证等。在证据审查阶段，举证方只需将电子数据、哈希值等上传至相关系统平台，就可以通过算法程序自动完成审查比对；法官通常依据算法程序的比对结果来认定电子数据的真实性，这无疑会降低审查中的主观性和裁量性，增强审查的中立性、客观性，从而更有利于实现鉴真效果。传统鉴真方法则建立在人对证据状态、特征等的感知之上，受制于人的认识、记忆和表达能力等因素，主观性较强，而这会影响对实物证据的鉴真效果。

其二，通过“保管链证明”“独特性确认”方法对实物证据进行鉴真，需由证据提供方承担证明责任，但电子数据技术性鉴真中通常采取“真实性推定”的方法，这使得相对方需承担一定的举证责任。2019 年最高人民法院《关于民事诉讼证据的若干规定》（以下称“民事诉讼证据规定”）第 94 条规定了电子数据“推定真实”的六种情形，其第 1 款第 2 项就涵盖了附有数字签名或采用类似安全保障技术认证的电子数据。〔40〕“互联网法院审理案件规定”第 11 条第 2 款、“在线诉讼规则”第 16 条分别规定，采用数字签名、可信时间戳、哈希值校验、区块链存证等技术手段收集固定的电子数据具有“推定真实”的效力。根据推定的一般原理，在满足对基础事实的证明要求之后可以认为推定事实成立，此时证明责任就转移至相对方，由相对方提供推定事实不真实的证据。〔41〕

域外也有类似的制度设计。美国《联邦证据规则》将实物证据的鉴真区分为“外部鉴真”和“自我鉴真”两类，分别受第 901 条、第 902 条调整和规范。前者由实物证据提供方承担证明责任，需要证明其提供的证据就是其主张的证据；后者则无需举证方提供证据证明实物证据的真实性。〔42〕在自我鉴真规则之下，需要由反对自我鉴真文件的当事人就其真实性问题承担举证责任。〔43〕为降低电子数据的鉴真难度和运行成本，2017 年，美国《联邦证据规则》第 902 条增设了第 13 项、第 14 项两项内容，它们分别是经认证的电子系统或程序记录、经认证的电子数据复制件，可借助哈希值比对以及其他能保障数据真实性的信息技术来实现电子数据自我鉴真。这些新的自我鉴真方法并没有改变电子数据鉴真的功能和标准，但影响了电子数据鉴真中的举证责任分配。〔44〕在新的自我鉴真规则之下，对于采用哈希值比对、区块链存证等技术认证的电子数据，举证方无需提供认证之外的证据，而需要相对方就电子数据不真实承担举证责任。此种消极性事实的证明难度较高，这会降低相对方就电子数据真实性提出异议的成功率和积极性。〔45〕

其三，借助“保管链证明”“独特性确认”方法完成对实物证据的鉴真，通常需要相关证人或在证据流转环节接触过实物证据的人出具证言证明证据的同一性和真实性；此时就需要证人出庭辨认实物证据，或者由相关人员出庭陈述证据收集、移送、保管等情况，相对方则可就证人或相关人员的陈述进行反询问。由于我国刑事司法中证人出庭率较低，实物证据的鉴真主

〔40〕 参见最高人民法院民事审判第一庭编著：《最高人民法院新民事诉讼证据规定理解与适用》下，人民法院出版社 2020 年版，第 826 页。

〔41〕 参见张保生：《推定是证明过程的中断》，《法学研究》2009 年第 5 期，第 177 页。

〔42〕 参见［美］罗纳德·J. 艾伦等：《证据法》，张保生等译，高等教育出版社 2006 年版，第 214 页以下。

〔43〕 参见前引〔12〕，奥伦斯坦书，第 226 页。

〔44〕 参见前引〔13〕，Grimm 等文，第 41 页。

〔45〕 参见前引〔20〕，Schupanitz 等文，第 112 页。

要借助相关笔录证据。庭审中，控方应出示并宣读实物证据的取证笔录，辩方可以就取证笔录提出异议。法官对证人证言或取证笔录的审查，主要建立在直接接触证人证言、取证笔录，听取质证意见之上。因此，传统鉴真方法的有效运行，需要完善的保管记录制度、证人出庭制度、质证辩论制度等作为支撑，对正当程序的要求较高。

电子数据技术性鉴真主要借助算法程序、数据代码等技术手段来实现电子数据同一性和真实性的证明与认定，在此过程中，通常仅需举证方操作相关技术设备进行演示，当场展示对相关数据的比对结果，而不需要借助证人或收集保管人对证据及其特征、保管情况的陈述。相对方就电子数据鉴真情况进行反驳，则围绕技术设备的可靠性、系统平台的主体资质等展开。因此，电子数据技术性鉴真对取证记录、证人出庭等制度的要求不高，但要求具备展示和运行数据比对的各种软硬件设施。但是，在电子数据技术性鉴真中，由于法官主要依据相关主体出具的认证材料来认定电子数据的真实性，而法官对保障电子数据真实性的技术方法缺乏直接感知，从而会在一定程度上减损电子数据审查中的正当程序保障。在美国的司法实践中，电子数据技术性鉴真也面临正当程序方面的质疑。比如，有学者认为，美国《联邦证据规则》第 902 条第 13 项、第 14 项在刑事案件中的适用，会侵害美国宪法第六修正案赋予被告人的对质权。〔46〕在依据上述规则以认证代替证人证言对电子数据进行鉴真时，并不需要就哈希值比对、区块链存证等技术方法出具认证的人员出庭作证，因为此种认证仅是对信息技术运行结果的确认，其中并不存在认证人员的判断或意见，出具认证的人员无需出庭接受质证。〔47〕此种争议就体现了电子数据技术性鉴真所引发的正当程序方面的问题。

五、电子数据技术性鉴真的制度整合与适用边界

信息技术可以高效、便捷实现对电子数据的鉴真，但是其适用也存在限度，这既源于信息技术自身的特点和局限，也源于鉴真规则在证据法体系中的功能和地位。“电子数据规定”“互联网法院审理案件规定”“在线诉讼规定”等规范性文件，已经勾画出电子数据技术性鉴真的制度雏形，现在有必要整合既有制度并构建电子数据技术性鉴真规则体系。

其一，应先确立我国的实物证据鉴真规则，然后在实物鉴真规则的基础上创设电子数据技术性鉴真规则。“互联网法院审理案件规定”“在线诉讼规则”等规范性文件虽然承认以区块链等技术方法收集固定的电子数据具有“推定真实”的效力，但在缺乏体系性实物证据鉴真规则的情况下，此类规定不仅显得较为突兀，而且无法对此处的“真实性”作出科学解释。我国现有证据制度并未明确规定鉴真规则，但其要义在现有证据制度中已经得到零星体现。比如，“民事诉讼证据规定”第 92 条第 1 款要求，由主张以私文书证证明案件事实的当事人，对私文书证的真实性承担举证责任。这是对鉴真中证明责任的规定。“电子数据规定”第 8 条、第 14 条至第 16 条、第 24 条要求在收集电子数据时制作取证笔录、录音录像，并要求在证据审查中依据这些笔录审查电子数据的来源、收集过程，这实际上确立了以笔录证据为基础的“证据保管链”鉴真方法；第 27 条、第 28 条也规定了未以封存状态移送、无法确定真伪

〔46〕 See Michael L. Levy & John M. Haried, *Practical Considerations When Using New Evidence Rule 902 (13) to Self-Authenticate Electronically Generated Evidence in Criminal Cases*, 67 DOJ Journal of Federal Law and Practice 88 – 93 (2019).

〔47〕 参见前引〔13〕，Grimm 等文，第 46 页以下。

等情形下，对电子数据的裁量排除和绝对排除，这实际上体现了电子数据鉴真不能的规范后果。

有必要系统梳理现有司法解释和规范性文件，从以下几个方面构建我国的实物证据鉴真规则：（1）明确鉴真责任主体是提供实物证据证明案件事实的当事人或检察机关。（2）鉴真对象包括物证、书证、视听资料、电子数据等实物证据。（3）对鉴真方法可以采取“列举 + 兜底”式规定，在鉴真方法中区分外部鉴真和推定鉴真。对于外部鉴真，需要实物证据提供方承担证明责任；对于推定鉴真，则采取形式真实性推定，主要通过证据自身特征、结构性要素或技术方法来保障实物证据的真实性。（4）设置实物证据鉴真标准，即鉴真仅解决实物证据的证据能力问题，其证明标准不宜设置过高，可采取优势证据标准。

在形成体系化的实物证据鉴真规则之后，可在此基础上创设电子数据技术性鉴真规则：（1）明确可以用来对电子数据进行鉴真的技术方法，对此也应采取“列举 + 兜底”式规定，从而保持技术性鉴真方法的开放性。（2）将技术性鉴真纳入电子数据推定鉴真范畴，赋予其“推定真实”的规范效力，其“推定真实”效果主要源于区块链存证等技术方法为电子数据真实性所提供的技术性保障。（3）相对方有权就技术方法的可靠性提出质疑。

其二，技术性鉴真仅适用于电子数据，而不适用于电子数据的存储介质或设备。电子数据取证有“一体收集”“单独提取”和“转化收集”三种模式。“一体收集”是将电子数据连同其原始存储介质一并予以收集、封存、移送；“单独提取”是仅收集提取电子数据而不扣押收集其原始存储介质；〔48〕根据“电子数据取证规则”第 8 条的规定，“转化收集”是将电子数据所承载的证据信息通过打印、拍照或录像等方法进行固定、收集，而不收集电子数据本身。

从技术性鉴真方法的适用范围看，其主要适用于“单独提取”模式，在“转化收集”模式中的适用具有限制性，在“一体收集”模式中的适用则具有阶段性。“电子数据取证规则”第 16 条、第 23 条、第 41 条中分别规定的现场提取电子数据、网络在线提取电子数据、调取电子数据，是“单独提取”的主要形态。公安机关采取这些侦查措施收集电子数据时，不仅要制作取证笔录，还要计算、记录完整性校验值。在“转化收集”模式中，电子数据承载的证据信息已被复制、固定在具有物质形态的照片或打印件上，故无法通过完整性校验等技术方法对电子数据本身进行鉴真，但可以通过笔录等方式形成证据保管链以保障电子数据的真实性。“转化收集”也可以通过录屏、录像等方式进行，此时应计算录屏录像视频的完整性校验值，并在取证笔录中予以记载。〔49〕不过，此时的鉴真对象已经变成取证后的示意证据而非原始电子数据。“电子数据取证规则”第 10 条中规定的扣押、封存原始存储介质是“一体收集”模式的典型情形。“一体收集”需要扣押、封存原始存储介质和提取电子数据两个步骤，在扣押、封存原始存储介质时，不需要计算完整性校验值，在提取电子数据时则需要计算完整性校验值。因此，技术性鉴真方法在“一体收集”模式中的应用具有阶段性。不难发现，技术性鉴真方法在适用范围上的局限，主要源于算法程序、数据代码等信息技术仅能对数字信息进行固定或处理，而不能适用于具有物质形态的电子数据存储介质或设备。

其三，电子数据的技术性鉴真方法既可以与传统鉴真方法交叉适用，也可以独立适用于电子数据鉴真。技术性鉴真方法通常不记载证据收集、移送、保管等环节的信息，通过技术性鉴

〔48〕 参见谢登科：《电子数据的取证主体：合法性与合技术性之间》，《环球法律评论》2018 年第 1 期，第 87 页。
〔49〕 参见前引〔17〕，刘浩阳等书，第 68 页以下。

真方法无法追溯或发现有关人员在收集、移送、保管等环节的不规范行为。因此，技术性鉴真方法在现阶段尚不能完全替代传统鉴真方法在规范侦查取证工作方面的功能，两种鉴真方法可以交叉适用，发挥各自所长。“电子数据规定”“电子数据取证规则”就主要采取交叉适用的方式，对电子数据既使用传统鉴真方法，也规定了技术性鉴真方法。比如，在电子数据的现场提取、在线提取、远程勘验中，除了要求制作取证笔录、见证人见证、同步录像外，也要求计算、记录完整性校验值。有学者也指出，虽然电子数据的真实性存在技术性保障，但电子数据在实践中仍会经过多个环节的流转迁移，若能辅以所有持有、接触、保管过该电子数据的人就电子数据的同一性和真实性向法庭提供令人信服的证言，以证明电子数据在流转环节得到妥善保管，则更能保障电子数据的真实性。〔50〕

随着算法取证、区块链存证等技术手段在电子数据取证中的使用，以及在线诉讼在司法实践中的逐步推广，技术性鉴真方法正逐渐从交叉适用向独立适用转变，即仅以区块链存证等技术方法来对电子数据进行鉴真。比如，区块链存证综合了分布式存储、非对称加密、时间戳等多项技术，在存证过程中会将电子数据哈希加密运算后分布存储在各个节点，生成时间戳，从而保障存证、流转的可追溯性，〔51〕这一防篡改、全程留痕、可追溯的特点，既可以为电子数据的同一性和真实性提供担保和证明，也可以追溯电子数据收集、保管等环节可能存在的瑕疵。因此，区块链存证技术在电子数据鉴真中的适用，可能会使技术性鉴真方法具有更强的独立适用性。“在线诉讼规则”“互联网法院审理案件规定”将区块链存证作为认定电子数据真实性之依据的规定，也为技术性鉴真方法的独立适用提供了制度依据。

其四，技术性鉴真仅能解决电子数据的同一性和形式真实性问题，而无法保障电子数据的实质真实性。鉴真规则属于证据能力规则而非证明力规则，证据能力主要解决证据是否具有准入资格的问题，而不解决证据是否具有证明力的问题。〔52〕而且，鉴真仅是影响实物证据之证据能力的因素之一，某一实物证据即便符合鉴真的要求，仍然有可能不被采信。因为鉴真仅是对出示证据与主张证据之同一性的确认，是对实物证据真实性的初步审查。对于通过区块链存证等技术方法进行鉴真的电子数据，也只是从形式真实性的角度解决电子数据的证据能力问题。此种形式真实性可以为保障电子数据的实质真实性奠定基础，但不能完全保障电子数据的实质真实性。对于电子数据的实质真实性，仍然需要由法官在证明力层面结合其他证据，运用生活经验、逻辑法则、良知理性等进行审查认定。

其五，在电子数据技术性鉴真的运行程序中，应保障诉讼主体的平等参与和有效对抗。电子数据技术性鉴真中可能存在的“技术偏在”“算法黑箱”等问题，会加剧控辩双方实力的差距与失衡，从而阻碍被告人正当程序权利的充分实现。比如，辩方难以知悉技术性鉴真的运行过程和机理；或者，即便控方披露或展示了技术性鉴真的算法和程序，辩方也可能因为欠缺信息技术和分析能力而无法对技术性鉴真进行有效质证。同时，在电子数据的技术性鉴真中，法官也可能因为缺乏技术知识储备而无法开展有效审查。以区块链存证为例，有实证研究表明，在已建立区块链存证平台的互联网法院，仅有 24.02% 的法官比较了解区块链技术，其他法院了解区块链技术的法官还不到 3%。〔53〕在对区块链技术缺乏必要了解的情况下，法官很难对

〔50〕 参见前引〔6〕，郭金霞文，第 65 页。

〔51〕 参见赵刚、张健：《数字化信任：区块链的本质与应用》，电子工业出版社 2020 年版，第 139 页。

〔52〕 参见孙远：《刑事证据能力导论》，人民法院出版社 2007 年版，第 6 页以下。

〔53〕 参见前引〔3〕，段莉琼等文，第 155 页。

区块链存证电子数据的技术性鉴真开展有效审查。

为了避免技术性鉴真的上述局限，需要在电子数据技术性鉴真中确立如下配套制度：（1）规范性文件赋予技术性鉴真的“推定真实”效力，会将举证责任配置给相对方，为了平衡此种责任分配效果，需要对举证方施加告知义务。对于通过区块链存证等技术手段收集、固定的电子数据，举证方应在提交证据时同步告知法院、对方当事人其采用的技术方法及认证情况，以为法院有效审查、相对方有效质证奠定基础。（2）我国在知识产权案件的诉讼程序中已经确立了技术调查官制度，技术调查官可以辅助法官审查、认定案件中的技术事实。可以在电子数据技术性鉴真中尝试引入技术调查官制度。（3）对于当事人，可以在电子数据技术性鉴真中考虑引入“有专门知识的人”制度。一方面，当事人有权申请有专门知识的人出庭辅助其就电子数据技术性鉴真问题进行质证和辩论。另一方面，对于数字弱势群体，如老年人、残障人士等，可以把他们纳入法律援助和司法救助范畴，指派有专门知识的人辅助他们就电子数据技术性鉴真问题进行质证和辩论。

Abstract: Authentication of electronic evidence is an important evidentiary issue in the age of information. In practice, information technologies such as integrity check value, trusted time-stamp, digital signature, and block-chain record are applied by judicial authorities in China in the authentication of electronic evidence. This is the result of the inability of traditional authentication methods, such as “chain of custody” and “uniqueness identification”, to effectively adapt themselves to the massive and virtual electronic evidence, as well as the institutional space created by the openness of the evidence authentication method system and the intrinsic demand created by the rapid development of online litigation. Technical authentication is not simply the application of information technologies to authentication of electronic evidence. It will bring about changes in the methods and rules of authentication of electronic evidence. Technical authentication methods and traditional authentication methods are not different in basic function and standard, but differ greatly in internal mechanism, burden of proof and procedural protection system. It is necessary to establish the rules of technical authentication for electronic evidence on the basis of integrating existing evidence rules. Technical authentication has its theoretical boundaries of application. It is mainly applicable to electronic evidence, but not the storage medium of electronic evidence. It can be applied alternately with traditional authentication, but there is a developing trend towards its independent application. It could solve the problem of only the formal, but not the substantive, authenticity of electronic evidence. In addition, it's necessary to protect equal participation and the right to confrontation of litigants in authenticating electronic evidence by technical methods.

Key Words: electronic evidence, authentication, integrity check, digital signature, block-chain record