

电子数据真实性的三层审查

载体、内容与来源：三重分解

赵跃

（安徽国运律师事务所，安徽 合肥 230000）

摘要：电子数据的真实性，实务中常被当作一个笼统的判断：或者整体采信，或者整体否定，很少区分究竟哪一层不真实。本文主张，真实性应分解为载体、内容与来源三层：载体真实性关注存储介质与运行环境是否可靠，内容真实性关注数据是否被增删改，来源真实性关注数据是否由所指向的主体生成并体现其意思。三层审查方法不同，证明责任亦不同。《最高人民法院关于民事诉讼证据的若干规定》第九十三条是审查方法，第九十四条是可反驳的推定，二者并非原则与例外，而是方法与推定的关系；实务将第九十四条当作确认清单，只要符合其一即予采信，且对“足以反驳”要求过高，致使推定近乎不可推翻。本文主张，反驳的门槛应是“具体说明篡改的可能性并指向具体环节”，而非证明篡改已经发生。就区块链存证而言，《人民法院在线诉讼规则》第十六条的推定仅及于上链后未经篡改，不及于上链前的真实性；上链前的真实性依第十八条由提交方证明。区块链提供的是完整性证明，而非真实性证明，这一区分应成为裁判说理的常识。

关键词：电子数据；真实性；载体；完整性；可反驳推定；区块链存证；具体否认义务

中图分类号：D925.1 **文献标识码：**A **文稿编号：**WJLT(2022)06-0014-12

Three Layers of Authenticity in Electronic Evidence: Medium, Content and Source

ZHAO Yue

(Anhui Guoyun Law Firm, Hefei 230000, Anhui, China)

Abstract: Authenticity of electronic evidence is often treated as a single all-or-nothing judgment, with little attention to which layer is actually disputed. This article argues that authenticity should be decomposed into three layers: the medium, concerning the reliability of storage devices and operating environments; the content, concerning whether the data has been altered; and the source, concerning whether the data was generated by the person it is attributed to and expresses that person's will. The three layers require different methods of examination and allocate the burden of proof differently. Article 93 of the Provisions on Evidence is a method of examination, whereas Article 94 creates rebuttable presumptions; the two stand in a relation of method and presumption, not principle and exception. Practice treats Article 94 as a checklist, admitting evidence once any item is satisfied and setting the threshold for rebuttal so high that the presumption becomes virtually irrebuttable. This article proposes that rebuttal should require only a specific account of how alteration was possible, pointing to a concrete step, rather than proof that alteration occurred. As for blockchain preservation, Article 16 of the Online Litigation Rules presumes only that data has not been altered after being uploaded, not that it was authentic before; pre-upload authenticity is governed by Article 18 and borne by the submitting party. Blockchain provides integrity, not authenticity, and this distinction should become commonplace in judicial reasoning.

Key words: electronic evidence; authenticity; medium; integrity; rebuttable presumption; blockchain preservation; specific denial

说明：（本文为作者个人研究观点，不代表所在单位意见）

作者简介：赵跃，安徽国运律师事务所执业律师，研究方向为证据法学、民事审判与在线诉讼。

电子数据已经成为民事审判中最常见的证据类型。微信聊天、电子邮件、电子合同、转账记录、监控视频、系统日志，几乎每一个合同纠纷、侵权纠纷都伴随电子数据。与之相对，对其真实性的审查却长期停留在一个笼统的判断上：要么整体采信，要么整体否定，判决理由中少见对“哪一层不真实”的具体分析。

笼统判断的后果是双重的。对于提交方，只要完成形式上的举证，数据往往被采信，

即使对方提出了具体的篡改疑点；对于异议方，欲推翻数据，须证明篡改已经发生，而篡改的痕迹通常已被技术手段抹去，证明几无可能。两端夹击之下，真实性审查或者流于形式，或者沦为举证能力的较量。

本文主张，真实性应当分解为载体、内容与来源三层。载体真实性关注存储介质与运行环境是否可靠；内容真实性关注数据是否被增删改；来源真实性关注数据是否由所指向的主体生成并体现其意思。三层的问题不同，审查方法不同，证明责任亦不同。混为一谈，必然导致判断的粗糙。

与此相关的是两部规范的理解。《最高人民法院关于民事诉讼证据的若干规定》（以下简称《民事证据规定》）第九十三条列举七项因素，第九十四条列举五种可以确认真实性的情形。通说将二者理解为原则与例外，本文则认为，前者是审查方法，后者是可反驳的推定，二者的适用顺序与法律效果均有区别。以下依次展开。

一、规范结构：方法、推定与顺序

（一）第九十三条是审查方法而非证明标准

第九十三条规定，人民法院对于电子数据的真实性，应当结合七项因素综合判断，包括系统环境是否完整可靠、是否处于正常运行状态、是否具备有效的防错监测手段、数据是否被完整保存传输提取、是否在正常往来活动中形成、保存传输提取的主体是否适当，以及影响完整性与可靠性的其他因素。

从文义看，该条提供的是判断的路径，而非判断的尺度。它告诉法官应当看什么，却未告诉法官看到何种程度可以认定真实。后者属于证明标准问题，由《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》第一百零八条确定，即高度可能性。将第九十三条误认为证明标准，会得出“七项因素均须具备”的结论，而该条使用的是“结合”，并非“同时具备”。

方法的意义在于，它使审查可以分项进行。法官可以逐项考察，指出哪一项存在缺陷、该缺陷对真实性的影响程度，而非笼统地认定“真实性存疑”。分项考察也使当事人知道应当针对哪一项举证，避免举证的无的放矢。

（二）第九十四条是可反驳的推定

第九十四条规定，电子数据存在五种情形之一的，人民法院可以确认其真实性，但有足以反驳的相反证据的除外。五种情形分别是：由当事人提交或者保管的于己不利的电子数据；由中立第三方平台提供或者确认的；在正常业务活动中形成的；以档案管理方式保管的；以当事人约定的方式保存传输提取的。第二款进一步规定，经公证机关公证的，应当确认真实性，但有相反证据足以推翻的除外。

这一结构是典型的可反驳推定：基础事实（符合五种情形之一）成立，推定事实（真实）成立，反驳由对方承担。推定之所以成立，是因为五种情形均具有较低的被篡改可

能：于己不利的数据，当事人无篡改动机；中立平台的数据，当事人无篡改机会；正常业务活动与档案管理形成的数据，有制度约束；约定方式保存的数据，有当事人合意。

关键在于“可以确认”与“足以反驳”的表述。前者表明推定并非强制，法院仍可结合具体情况不予确认；后者表明反驳无须达到“排除合理怀疑”，只须足以动摇推定的基础。实务中常将“足以反驳”理解为“证明数据已被篡改”，这一理解抬高了门槛，使推定近乎不可推翻。

（三）适用顺序

两条规范的适用顺序是：先依第九十三条审查，判断数据在三层上是否存在缺陷；符合第九十四条情形之一的，可以直接推定真实，无须逐项审查；对方提出反驳的，再回到第九十三条的方法，就争议的层次具体审查。顺序颠倒，会导致两个极端：先推定后审查，使第九十三条被架空；不适用推定而逐项审查，使审查成本过高。

还需注意，第九十四条的五种情形与第九十三条的七项因素并非一一对应。前者着眼于数据的形成与保管机制，后者着眼于技术与环境。故在适用推定时，仍须确认基础事实的存在，如“中立第三方平台”是否确实中立、“正常业务活动”是否确实存在。基础事实不成立的，推定无从适用。

电子证据在诉前的固定方法，包括原始载体保管、完整对话的导出、公证与可信时间戳的运用，实务中的具体步骤可参见“电子证据如何有效固定”一文的梳理；本文不重复取证的操作方法，只讨论进入诉讼后真实性审查的层次与证明责任。

（四）三层与证据三性的关系

证据的合法性、真实性与关联性，通常被称为三性。三层分解并不取代三性，而是把其中的真实性一层展开。合法性关注取得手段是否合法，如是否侵犯他人隐私、是否违反程序规定；关联性关注数据与待证事实之间的联系；真实性关注数据本身是否可靠。三者之中，真实性最易被笼统处理，因为它不像合法性那样有明确的标准，也不像关联性那样可以直观判断。

三层分解与三性的关系，可以概括为：合法性是前提，真实性是基础，关联性是桥梁。取得手段违法的数据，即使真实也不得使用；真实但与待证事实无关的数据，不具有证明价值；关联性强但真实性存疑的数据，须补强后方可使用。三个层次的审查不可互相替代，尤其不可用关联性的强弱替代真实性的判断。

（五）完整性与真实性的区别

完整性指数据未被增删改，真实性指数据反映了客观事实。二者相关但不等：完整的数据可能是虚假的，如当事人如实记录了一个虚假的交易；不完整的数据也可能反映真实，如截取的片段恰好是核心内容。审查时须先判断完整性，再判断真实性，不能以完整性代替真实性。

这一区分在区块链存证中尤为重要。区块链能够保证数据上链后不被修改，从而保证完整性；但上链前的数据是否真实，区块链无从判断。若当事人将一份伪造的合同上链存证，区块链只是证明了该合同自某时起未被修改，不能证明合同是真实签订的。混淆二者，等于把技术能力误认为证明力。

二、三层分解：载体、内容与来源

（一）载体真实性

载体真实性，指存储电子数据的介质与运行环境是否可靠。审查的对象是设备、系统、网络与存储过程。具体包括：设备是否为当事人主张的设备；系统是否处于正常运行状态；存储过程是否有日志记录；数据是否被完整地提取与固定。

载体不真实的典型情形，是数据并非来自所主张的设备。例如，当事人主张微信聊天记录来自其本人手机，但提取时使用的却是他人手机；或者主张系统日志来自公司服务器，但服务器在争议期间曾经更换。此类情形，数据的来源即不可靠，无论内容是否完整，均不应采信。

载体的审查，通常需要技术手段。法院可以要求当事人当庭演示原始载体，可以委托鉴定或者勘验，也可以要求提交方提供提取过程的录像或者公证书。当事人无正当理由拒不提供原始载体的，可以依《民事证据规定》第九十五条，作出对其不利的认定。

（二）内容真实性

内容真实性，指数据本身是否被增删改。审查的对象是数据的完整性，包括：数据是否完整、是否存在截取、拼接、编辑的痕迹、时间戳是否连续、哈希值是否一致。完整性与真实性不是同一概念，但不完整的数据往往不可靠。

微信聊天记录的完整性，尤为关键。截取片段的聊天记录，可能遗漏了前后文，导致语义反转；删除部分消息的，可能改变了当事人的意思。故审查时应要求提交完整的对话，包括时间、参与人、上下文。仅提交对自己有利的片段，又无合理解释的，不宜采信。

内容真实性的证明，可以通过技术手段完成。哈希值比对是最常用的方法：数据生成时计算哈希值并保存，争议时重新计算，二者一致即可认定未被篡改。区块链存证即以此为基础。此外，公证、时间戳、第三方存证平台的确证，均可作为完整性的证明。

（三）来源真实性

来源真实性，指数据是否由所指向的主体生成，是否体现其意思。这是三层中最易被忽视、也最常成为争议焦点的一层。载体可靠、内容完整，并不等于数据由对方生成：账号可能是共用的，设备可能是借用的，邮件可能是代发的。

来源真实性的审查，须结合账号归属、设备控制、交易背景综合判断。微信账号的归

属，可以通过实名认证信息、绑定手机号、朋友圈内容、交易记录确定；电子邮件的来源，可以通过发件服务器记录、签名、往来习惯确定；电子合同的签署，可以通过实名认证、数字证书、短信验证码确定。

实务中一种常见的错误，是以“内容提到了对方”“对方未否认”推定来源真实。此类推定缺乏基础：内容提及他人，任何人都可以做到；未予否认，可能出于不知情或者不屑回应。正确的做法是要求提交方就账号归属、设备控制举证，对方否认的，由其就否认举证。

三、推定与反驳的具体操作

（一）反驳的对象

反驳应当针对具体的层次。对方主张载体不真实的，应当指出设备、系统或者提取过程中的具体问题；主张内容不真实的，应当指出增删改的具体位置或者技术可能；主张来源不真实的，应当指出账号、设备或者签署环节的具体疑点。笼统主张“数据可以伪造”，不构成有效的反驳。

这一要求称为“具体否认义务”。其法理在于，电子数据的真实性涉及专业判断，若允许笼统否认即启动审查，则任何电子数据都将陷入无休止的争议。要求具体否认，既保障了异议方的权利，又避免了程序的空转。

具体否认的证明程度，无须达到“证明篡改已经发生”，只须“说明篡改的可能性并指向具体环节”。例如，指出提交方在争议发生后曾多次登录系统、数据文件的修改时间晚于生成时间、聊天记录的发件时间与设备时区不符。这些事实足以动摇推定的基础，审查即应展开。

（二）反驳成立后的后果

反驳成立，推定的效果消失，但并不等于数据不真实。此时举证责任回到提交方，其须依第九十三条逐项证明真实性。提交方不能证明的，数据不予采信；能够证明的，仍可采信。这一分配体现了推定的相对性：推定只是暂时转移举证负担，而非终局确定事实。

实务中常将反驳成立等同于数据不真实，径行排除。这一处理简化了程序，却可能排除真实的数据。正确的做法是，在反驳成立后给予提交方补充举证的机会，如提交原始载体、申请鉴定、提供第三方存证的确证。未经此步骤径行排除，属于程序上的草率。

（三）推定不适用的情形

第九十四条第一项的“于己不利”，须作实质判断。当事人在诉讼中提交的数据，若整体上对其不利，可以推定真实；但若数据中部分不利、部分有利，而当事人仅提交有利部分，则不属于该项情形。判断的标准，是数据在整体上是否违背提交方的利益，而非其中是否含有不利的片段。

“正常业务活动”的判断，须考察数据的形成是否属于业务常规。日常的订单、发货、对账记录，属于正常业务活动；为诉讼目的专门制作的汇总表、说明材料，不属于。后者虽由系统生成，但其形成具有明确的诉讼目的，可靠性低于日常记录，不能直接适用推定。

（四）公证的效力及其界限

经公证的电子数据，依第九十四条第二款应当确认其真实性，但有相反证据足以推翻的除外。公证的效力强于一般推定，原因在于公证机构在取证时进行了现场监督与记录，其证明力较高。但公证并非绝对，若有证据表明公证程序存在瑕疵，如取证时未核对设备、未记录完整过程，仍可推翻。

公证的效力范围，限于公证书记载的取证过程与数据状态。公证之后数据是否被篡改，公证无从证明。故对方主张公证后数据被修改的，仍应审查。实务中常以“已经公证”一语排除全部异议，这一处理超出了公证的效力范围。

四、区块链存证的效力边界

（一）第十六条的推定范围

《人民法院在线诉讼规则》第十六条规定，当事人提交的电子数据系通过区块链技术存储，并经技术核验一致的，可以认定该数据上链后未经篡改，但有相反证据足以推翻的除外。这一推定的范围有明确限定：仅及于“上链后未经篡改”，不及于上链前的真实性，也不及于数据内容的真实。

这一限定常被误读。实务中，当事人提交区块链存证证书，主张数据真实，法院亦有直接采信者。此种处理混淆了完整性与真实性：区块链能够证明的是，上链时的数据与现在提交的数据一致；不能证明的是，上链时的数据本身是否真实。若上链时数据已经是伪造的，区块链只是忠实地保存了伪造的数据。

因此，区块链存证的证明力，应表述为“完整性推定”而非“真实性推定”。判决理由中应当写明：该数据上链后未经篡改，可以认定其完整性；至于上链前是否真实，须另行审查。这一表述的精确性，直接影响到当事人的举证方向。

技术核验的操作，通常是重新计算提交数据的哈希值，与链上存储的哈希值比对。二者一致的，可以认定数据自上链时起未被修改。核验应当在庭审中当庭进行，或者由双方共同委托的机构进行，以避免单方操作引发的争议。当事人对核验结果有异议的，可以申请鉴定。

还须区分存证时间与事实发生时间。区块链记录的是数据上链的时间，这一时间通常晚于事实发生的时间。存证平台出具的证书，只能证明“某时点该数据已经存在”，不能证明“该数据所记载的事实发生于该时点”。实务中常以存证时间作为事实发生时间，这一推定缺乏依据，须有其他证据印证。

（二）上链前真实性的审查

《人民法院在线诉讼规则》第十八条规定，当事人提出数据上链存储前已不具备真实性，并提供证据证明或者说明理由的，法院应当审查；法院可以要求提交方证明上链前数据的真实性，并结合数据来源、生成机制、存储过程、公证、第三方见证、关联印证等情况综合判断；提交方不能证明或者合理说明，且数据无法与其他证据印证的，不予确认真实性。

该条实际上把上链前真实性的举证责任分配给了提交方，且以“不能证明或者合理说明”为不利后果的条件之一，同时要求数据无法与其他证据印证。两个条件并列，意味着即使提交方不能充分证明，只要数据能与其他证据印证，仍可采信。这一安排体现了印证的补强作用。

审查上链前的真实性，应着重三个方面：数据从何而来，是交易系统自动生成还是人工录入；生成机制是否可靠，有无防错设计；存储过程是否连续，有无中断或者转存。三者之中，自动生成的数据可靠性最高，人工录入的数据须有原始凭证印证。

（三）平台资质与利害关系

第十七条规定了异议成立后的四项审查因素，包括存证平台是否符合国家有关规定、当事人与平台是否存在利害关系并利用技术手段不当干预、平台系统是否符合清洁安全可靠可用的标准、存证技术与过程是否符合国家标准或者行业标准。四项因素中，第二项最具实践意义。

当事人与存证平台存在利害关系，是区块链存证的常见软肋。若平台由提交方自行搭建或者控股，其“中立第三方”的地位即不成立，存证的时间戳、哈希值均可能被预先设定。此时即使技术核验一致，也不能认定上链后未经篡改，因为篡改可能发生在“上链”这一动作本身。

审查的方法是要求提交方说明平台的投资关系、实际控制人、服务协议。提交方不能说明或者说明显示存在关联的，应认定存证的中立性不足，转而要求其提供其他证据印证。这一审查并不苛刻，因为合规的存证平台本应保持独立，关联关系的确存在本身即构成合理的怀疑。

五、典型电子数据的审查要点

（一）即时通讯记录

即时通讯记录的审查，三层均易生争议。载体层面，须确认提取自哪一设备、设备由谁控制、是否为原始载体；内容层面，须确认对话是否完整、有无删除、时间是否连续；来源层面，须确认账号归属、发送人身份。三层之中，来源最为关键，因为账号的实名信息与实际使用人常不一致。

审查的方法，可以要求提交方当庭登录账号、展示通讯录与聊天窗口、演示搜索过程。对方对账号归属有异议的，可以申请调取运营商的实名信息。实践中还有一种情形，即当事人使用他人身份注册的账号，此时须结合手机号、绑定银行卡、交易习惯综合认定。

群聊记录的审查更为复杂。群成员的身份、发言的上下文、是否经过编辑，均须查明。仅截取群聊中的一段发言，未显示发言人身份的，不足以认定该发言出自特定主体。故提交群聊记录，应当同时提交群成员列表与完整的上下文。

（二）电子邮件与电子合同

电子邮件的审查，重点在来源。发件人的邮箱地址、发件服务器的记录、邮件的数字签名，均可用以确定来源。仅有邮件正文而无邮件头信息的，来源难以确定；转发件、打印件的证明力更弱。实务中，法院可以要求提交方提供原始邮件或者申请调取服务商的记录。

电子合同的审查，重点在签署环节。可靠的电子签名须满足专有性、可控性、可检测性三项要求，其效力由电子签名法规定。审查时应当确认：签署主体是否经过实名认证；签署时是否使用了数字证书；签署后的合同是否被修改；存证平台是否记录了签署过程。四项具备的，可以认定合同成立且内容真实。

实务中常见的情形是，当事人仅提交电子合同的截图或者打印件，未提交签署过程的记录。此时合同的真实性难以确认，尤其是对方否认签署的场合。故电子合同的提交，应当包括合同文本、签署记录、实名认证信息、时间戳四项材料。

（三）监控视频与系统日志

监控视频的审查，重点在完整性与连续性。视频是否经过剪辑、时间是否连续、画面是否清晰、拍摄角度是否能够反映争议事实，均须查明。仅有片段而无原始存储介质的，证明力较弱；原始介质中的视频被覆盖的，应当说明覆盖的原因与时间。

系统日志的审查，重点在生成机制。日志由系统自动生成，通常具有较高的可靠性，但须确认系统未被篡改、日志未被删除、时间戳准确。审查时可以要求提交方说明系统的架构、日志的存储周期、访问权限的分配。必要时可以委托鉴定。

（四）网页与电子公告

网页证据的审查，难点在可变性。网页内容随时可以修改或者删除，而当事人提交的往往是截图或者打印件，无法反映原始状态。审查时应当确认：取证的时间；取证的方式，是直接截屏还是通过公证、时间戳固定；网页的网址、域名归属；内容是否完整，有无遗漏导航栏、页脚、发布时间。

较为可靠的方式，是申请公证或者使用可信时间戳固定网页。公证书记载了取证的时间与过程，证明力较高；可信时间戳由第三方机构签发，能够证明某文件在某一时间点已经

存在。二者的共同点，是把“取证时点的状态”固定下来，从而使后续的争议有据可查。

对于电子商务平台的交易记录、商品页面，可以要求平台提供后台数据。平台作为第三方，其数据具有较高的可靠性，属于第九十四条第二项所规定的“中立第三方平台提供或者确认”。当事人仅提交自行截图的页面，对方否认的，证明力较弱。

（五）电子病历与医疗数据

医疗纠纷中的电子病历，具有专业性与封闭性。其由医疗机构的信息系统生成、存储，患者一方无从接触。审查时应当注意：病历是否及时形成，有无事后补录；修改痕迹是否保留，有无删除；电子签名是否完整；系统时间是否准确。

依《医疗纠纷预防和处理条例》与相关规范，医疗机构应当妥善保管病历，不得篡改、伪造、隐匿、销毁。患者一方对病历真实性提出异议并说明理由的，医疗机构应当就病历的形成过程举证。不能举证的，可以推定病历存在瑕疵，进而影响其证明力。这一分配，与电子数据三层审查的思路一致：控制数据的一方，负较重的证明责任。

（六）其他可信固证方式的比较

区块链之外，常见的固证方式有公证、可信时间戳、第三方存证平台的电子签名存档、司法鉴定。四种方式的证明力依次递减，但均高于当事人自行保存的原始数据。选择何种方式，取决于争议金额、数据的复杂程度与对方的抗辩可能，不能一概而论。

公证的优势在于有公证员现场监督，程序规范，证明力最强，缺点是成本较高、手续较繁。可信时间戳的优势在于成本低、速度快，能够证明某文件在某一时点存在，缺点是无法证明取证过程是否规范。第三方存证的优势在于自动化，缺点是与平台的中立性密切相关。司法鉴定可以解决技术争议，但只能在争议发生后进行，且鉴定对象受限于提交的材料。

实务中宜采分层策略：争议金额大、对方抗辩激烈的，宜采公证；日常交易、金额不大的，可信时间戳即可；系统自动生成的业务数据，宜由平台方出具确证。分层策略的意义，在于使固证成本与争议价值相匹配，避免小案大办，也避免大案轻办。

（七）跨境电子数据的取证

跨境交易中的电子数据，取证涉及司法协助与数据出境。当事人自行从境外服务器下载的数据，其完整性与来源均难以确认，对方常以此抗辩。较为可靠的方式，是通过司法协助请求境外机构调取，或者由境外公证机构公证后转递。两种方式耗时长，但在争议金额较大时仍有必要。

数据出境的问题，须依数据安全法与个人信息保护法的规定处理。法院要求当事人提交存储在境外的数据，可能涉及数据出境的审批。实务中宜优先要求当事人提交其在境内留存的数据，或者要求境外一方通过合法途径提供。径行要求提交境外数据而不考虑合规要求，可能使当事人陷入两难。

对于境外平台生成的交易记录，可以要求平台方出具书面确证，并附公证认证。平台的的确证属于第九十四条第二项的“中立第三方平台提供或者确认”，具有推定的效力。对方有异议的，应当具体说明平台不中立或者数据被修改的理由。

六、裁判技术的展开

（一）举证责任的分配与告知

电子数据的举证责任，原则上由提交方承担。其须证明数据来源于所主张的设备或者系统、内容完整、由所指向的主体生成。对方否认的，须具体说明否认的理由，此为具体否认义务。法院应当在庭审中明确告知双方各自的举证内容，避免一方因不熟悉规则而失利。

对于符合第九十四条情形的，法院可以告知提交方无须逐项举证，同时告知对方可以在指定期限内提出具体反驳。这一告知使推定与反驳的规则得以运行，也避免了庭审的反复。未告知而运行认定推定成立，属于程序上的不足。

（二）说理的结构

说理应分三层展开。第一层认定载体，说明数据提取自何设备、由谁控制、提取过程是否规范；第二层认定内容，说明数据是否完整、有无篡改痕迹、哈希值是否一致；第三层认定来源，说明账号归属、签署主体、生成机制。三层均无缺陷的，认定真实；某一层存在缺陷的，说明该缺陷对整体真实性的影响。

对于不予采信的数据，应当说明具体理由，而非笼统写“真实性无法确认”。例如，“该微信聊天记录系截取片段，未显示前后文，且提交方未能当庭登录原始账号，账号归属无法确认，故不予采信”。此种说理使当事人知道败在何处，也为类案提供参照。

（三）技术辅助的运用

电子数据的审查具有专业性，法院可以依当事人申请或者依职权委托鉴定，也可以通知有专门知识的人出庭。鉴定的事项应当具体，如“该文件是否经过编辑”“该时间戳是否被修改”“该哈希值与提交的数据是否一致”，而非笼统的“是否真实”。

有专门知识的人出庭，其意见视为当事人的陈述，不属于鉴定意见，但可以帮助法院理解技术问题。法院在采信时应当说明理由，不能仅以“专家认为”代替论证。对于双方各自聘请的专家意见相反的，应当结合其他证据判断，必要时另行委托鉴定。

（四）自认与证据契约

当事人对电子数据的真实性明确表示认可的，构成自认，法院可以直接采信，无须再作审查。自认可以明示，如当庭表示认可；也可以默示，如对对方提交的数据不发表质证意见。但涉及国家利益、社会公共利益或者他人合法权益的，自认的效力受限制。

当事人也可以就电子数据的真实性达成证据契约，如约定某平台的数据推定为真实、约定以哈希值比对作为唯一标准。此类契约只要不违反法律强制性规定与公序良俗，应当尊重。契约的存在，可以简化审查，但也可能被一方利用，故法院应当审查契约是否显失公平、是否存在重大误解。

（五）二审的审查重点

二审对电子数据真实性的审查，应当尊重一审的认定，除非存在明显错误。一审已经组织当庭演示、鉴定或者勘验的，二审原则上不再重复；一审仅凭书面材料认定的，二审可以要求补充演示或者提交原始载体。审查的重点，是一审是否就三层分别作出认定，是否遗漏了当事人的具体反驳。

对于一审未说明理由即采信或者排除的，二审应当指出说理不足。可以补充查明后改判，也可以发回重审。选择的标准是：事实是否已经查清。若关键事实需要当庭演示或者鉴定，宜发回；若仅需补充说明，可以改判。

（六）不予采信的后果与替代路径

电子数据不予采信，不等于待证事实不能成立。当事人仍可以通过其他证据证明同一事实，如书证、证人证言、当事人的陈述结合其他间接证据。法院在排除某份电子数据时，应当说明其他证据是否足以支撑待证事实，不能因一份数据被排除即径行驳回全部请求。

反之，电子数据被采信，也不等于待证事实当然成立。数据只能证明其记载的内容，内容与待证事实之间的关联，仍须依经验法则判断。例如，转账记录可以证明款项的交付，但不能证明款项的性质是借款还是货款，后者须结合聊天记录、合同、交易习惯综合认定。

七、结语

电子数据的真实性，不是一个可以用“真”或者“假”回答的问题。它是一组分层的问题：数据来自何处，是否完整，由谁生成。三层各自成立，整体才真实；任何一层存在缺陷，整体的可靠性即受影响。把三层压缩为一个判断，必然导致审查的粗糙与说理的空洞。

据此，第九十三条应被理解为分层的审查方法，第九十四条应被理解为可反驳的推定。推定的效果是转移举证负担，而非终局确定事实；反驳的门槛是具体说明篡改的可能性，而非证明篡改已经发生。这一理解为异议方保留了实质的救济空间，也避免了推定的滥用。

区块链存证的效力，同样应当精确表述：它证明的是完整性，而非真实性；推定仅及于上链后，不及于上链前。这一区分看似技术，实则关乎当事人的举证方向：知道推定范

围的提交方，会注重上链前证据的固定；知道推定范围的异议方，会把攻击点放在上链前的环节。规则清楚，攻防才有意义。

最后须指出，电子数据的审查终究是证据判断的一部分，技术只是辅助。无论技术如何发展，判断的核心仍是经验与逻辑：该数据是否符合交易的习惯，是否与其他证据印证，是否能够解释其中的疑点。技术可以提供事实，但不能代替判断。裁判者的职责，是在技术提供的事实之上，作出符合常理与法律的评价。这一评价之所以不可替代，是因为它必须回应具体案件中当事人的处境与交易的常识，而任何技术标准都无法穷尽这种处境，也无法代替法官对证据分量的整体权衡。三层分解的意义，恰在于为这种权衡提供一个可以讨论、可以审查的框架。

参考文献

- [1] 《中华人民共和国民事诉讼法》第六十六条、第七十三条。
- [2] 《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》（法释〔2022〕11号）第一百零八条、第一百一十六条。
- [3] 《最高人民法院关于民事诉讼证据的若干规定》（法释〔2019〕19号）第九十三条、第九十四条、第九十五条。
- [4] 《人民法院在线诉讼规则》（法释〔2021〕12号）第十六条至第十九条。
- [5] 《中华人民共和国电子签名法》第十三条、第十四条。
- [6] 最高人民法院：《〈人民法院在线诉讼规则〉的理解与适用》，载《人民法院报》2021年6月17日。
- [7] 刘品新：《电子证据法》，中国人民大学出版社2021年版。
- [8] 谢登科：《区块链存证的真实性审查》，《法学》2022年第7期。