【电子文件】

基于区块链的电子证据保全模式研究

——以广州互联网法院为例

聂勇浩　张　炘

【摘　　要】网络诉讼的普遍化使得电子证据成为司法电子文件管理的重要对象，区块链不可篡改、可追溯和去中心化等技术特性为电子证据保全提供了新的思路。基于区块链技术，广州互联网法院构建了“网通法链”信用生态系统，以应对电子证据的可采、可信、可控和可用问题。本文从合法性、真实性、安全性和可用性四个维度归纳了广州互联网法院的电子证据保全策略，提炼出以司法认可、规范建设和规则输出策略保全合法性，以区块链全程监管、多阶段哈希值校验、多链聚合和多主体背书策略保全真实性，以哈希算法、非对称加密技术、分布式存储和系统防护机制保全安全性，以元数据抽取、格式转换、脱机存储和定期检测措施保全可用性的电子证据保全模式，并针对区块链性能瓶颈和可用性保全措施的局限性等问题，讨论了下一步的发展思路。

【关 键 词】电子证据；电子文件；证据保全；区块链

【作者简介】聂勇浩，张炘，中山大学信息管理学院（广州 510006）。

【原文出处】《档案学研究》（京），2021.5.28～36

【基金项目】本文系中山大学教学质量工程类项目“《档案管理学》中的中国特色与中国道路”的阶段性研究成果。

1 研究背景

为回应数字时代的涉网司法需求，我国在杭州、北京、广州都设立了互联网法院。不同于传统法院，互联网法院采用全流程网络化办理的诉讼新模式，涉诉文件从生成到归档均以数字形式存在，电子证据成为公众维护自身在网络空间中合法权益的重要凭证。[1]由于电子证据面临着易篡改、易消亡等问题，在管理过程中有效保全其证据资格和证据能力，对互联网法院诉讼业务的持续发展尤为重要。

但是，目前无论是理论还是实践层面，都尚未形成完整的电子证据保全框架。虽然有文献探讨了基于公证保全模式[2]或可信时间戳服务[3]的电子档案证据价值维护方案，但是对电子证据保全的研究明显不足。近年来，区块链技术由于其去中心化、不可篡改的技术特性，成为电子文件管理中极具应用潜质的前沿技术。通过积极推进区块链的深度应用，广州互联网法院在电子证据保全实践中取得了阶段性进展。论文以这一典型案例为研究对象，分析广州互联网法院基于区块链的电子证据保全实践，从而尝试归纳电子证据保全中值得借鉴和推广的普遍性模式。

2 文献综述

对于区块链技术在电子文件管理中的应用，现有文献集中于适用性、应用场景和应用案例三个方面。

首先，对于区块链在电子文件管理中的适用性，Lemieux[4]、Findlay[5]及刘越男[6]等阐述了区块链在维护电子文件真实性、完整性、隐私性和存储安全，提高档案管理效率和档案信息防篡改等方面的天然优势。不过，李高峰等[7]认为，区块链技术在电子文件管理上的应用受限于档案管理环境、技术瓶颈和应用经验等因素。Lemieux[8]指出链上电子文件存在被推翻的风险及完整性、长期保存和法律适用性等管

理难题。刘越男等[9]也剖析了区块链在数字档案长期保存方面的不足。

其次，区块链在电子文件管理中的应用场景是另一个较受关注的话题。从管理对象的角度，区块链技术为平衡电子医疗档案的高隐私性、可访问性和互操作性提供了途，径[10][11]，也能有效契合人事档案[12]、高校档案[13]等专门性电子档案的管理需求。从管理模式的角度，区块链为去中心化的分散存档机制和参与式的档案管理新模式提供了技术支持。[14]从管理环节的角度，则有对区块链应用模式[15]、存储模式[16]及社交媒体信息归档[17]、档案信息资源共享[18]、电子文件安全存储[19]和可信保护[20]等方面的研究。

最后，在应用案例上，国外研究介绍了英国ARCHANGEL方案[21]、洪都拉斯土地档案保存方案FACTOM[22]、档案系统ARCHAIN[23]等实践项目。国内研究当中，许海涛[24]则分析了杭州互联网法院司法区块链在电子证据可信判定中的应用。

总体而言，现有研究主要还是集中于区块链技术应用于电子文件管理的理论分析和案例介绍，针对电子证据保全的管理实践的研究，还有待于进一步加强。

3 核心概念与研究思路

3.1 电子证据和电子证据保全

电子证据是作为证据使用的电子数据的总称，是司法电子文件的重要类型之一。根据《最高人民法院、最高人民检察院、公安部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》(法发[2016]22号)等法律文本，电子证据指“在案件发生过程中形成的，以数字化形式存储、处理和传输的，能够证明案件事实”并用作证据使用的材料及其衍生物。互联网电子证据的保全包括对电子文件证据资格和证明能力的保障。[25]因此，电子证据保全指的是考虑到电子证据易篡改、易伪造、易受损和易消亡的特性[26]，采取一定措施提取、固定和保存电子证据，以规避电子证据失真、破损或灭失等风险，保障其证据资格和证据能力的一种电子证据管理活动。

值得一提的是，现有文献虽然存在将“电子存证”和“电子证据保全”概念混用的现象，但二者并非相互等同或互为替代的关系。存证是对数据的同步记录和留存以确保诉讼发生时的证据取得。电子证据保全和电子存证虽然都指向电子证据的提取和固定，却在时间和目的上有所区别。就时间而言，电子存证是一种瞬时性行为，一般发生在诉讼成立前的某个时间点；电子证据保全是一种持续性行为，贯穿电子证据整个生命周期。就目的而言，电子存证以电子证据的留存和取得为目的，旨在确保诉讼发生时有证据可用；电子证据保全则是为了保障电子证据的证据资格和证据能力，确保证据可以使用。

3.2 研究方法

本文采用单案例研究法对电子证据保全模式进行探索性研究。之所以选取广州互联网法院作为分析对象，主要是考虑到案例对象的典型性。广州互联网法院首创的“网通法链”信用生态系统，提供了可复制推广的电子证据保全创新模式和实践样本。在资料收集上，研究者基于电子证据保全的已有文献，从合法、真实、完整、安全、可用等角度设计了一个粗线条式的访谈提纲，对法院相关负责人展开面对面的半结构化访谈，并以其公众号推送内容和总结报告等文本为补充，形成研究的实证资料来源。

在资料分析上，研究者采用从具体到一般的归纳式思维开展内容分析。首先通过开放式编码从原始资料中提取出有效概念，其次归纳整合为主要范畴和更具概括性的类属，最后通过核心编码对已发现的类属关系进行系统分析，形成相应的理论观点，从而建立起广州互联网法院电子证据保全的理论框架。

3.3 分析框架

3.3.1 电子证据保全的基本要素

电子证据作为诉讼过程中形成的司法电子文件，兼具传统证据的功能特征和电子文件的基本特性。在证据法学中，一份证据的证据资格和能力以其合法性、真实性和关联性为依托。其中，证据真实性与文件的真实性、完整性和可靠性都有所关联；证据关联性作为证据的自然属性[27]，则取决于证据与待证事实间的逻辑联系，主要依靠法官的司法经验和逻辑判断而不涉及证据真假。因此，电子证据保全应当实现文件管理“四性”标准和证据“三性”特征

的属性对接，并充分考虑电子证据载体和生存环境的特殊性，达到合法性、真实性、安全性和可用性四大要素的动态平衡，具体如图1所示。

合法性是电子证据保全的前提和起点。传统意义上的证据合法性是指证据的主体、形式、获取方式和程序符合法律规定。电子证据的合法性一方面要求电子证据生成、收集、固定和存储等过程中的主体、工具和方式符合相关的法律要求和技术规范，另一方面要确保电子证据本身的合法、规范。

真实性是电子证据保全的核心和落脚点。电子证据的真实性比电子文件的真实性在内涵上更加广泛，可以说电子文件可靠、真实、完整三大属性共同指向司法意义上的电子证据真实性。[28]具体而言，电子证据的真实性包含内容真实和形式真实两层含义。内容真实是指电子证据能够客观、准确地反映其所要证明的事物或事实的能力，强调电子证据的内容是可信、可靠而非伪造或虚构的，与电子文件的可靠性要求趋同。形式真实强调“同一性”[29]，指电子证据与其最终形成时的状态保持一致，描述的是电子证据自形成后未经篡改或破坏的特性，与电子文件的真实性特征相近。

在完整性上，电子证据和电子文件的要求有所差异。就电子文件的完整性而言，首先是指每份电子文件的内容、结构、背景信息和元数据等相关要件没有缺失或破损，其次是指与某份电子文件具有有机联系的其他文件及相关文件是齐全完整的。司法层面对电子证据完整性的审查更强调微观层面的数据完整，表现为电子证据不受破坏、剪裁或非法修改的状态。电子证据完整性的实质是证据真实性的下位概念[30]，属于电子证据形式真实性的重要因素，可以通过对电子证据进行全生命周期的过程记录和痕迹管理，保障任何对电子证据的操作行为可追溯且不可抵赖来实现。[31]

安全性是证据保全在数字环境下的拓展和延伸。面对数字环境给电子证据带来的安全隐患，安全性指向电子证据在运行及存储过程中，规避非法访问与泄密风险、避免非法攻击和破坏造成的数据丢失或受损、维护系统持续运转和数据容灾容错的能力。

可用性是数字载体对电子证据保全提出的要求，指电子证据可以被查找、检索、呈现和理解的特性，既要满足用户对电子证据的查询和检索需求，也要确保电子证据随着系统的变化而迁移或转换，使其在规定期限内保持持续可用的状态。

3.3.2 广州互联网法院的电子证据保全模式

区块链技术并不是一种单一的技术，而是整合了区块链数据结构、区块链算法、密码学原理等多种技术的综合性技术应用模型。[32]广州互联网法院构建的以“一链两平台”为核心的“网通法链”信用生态

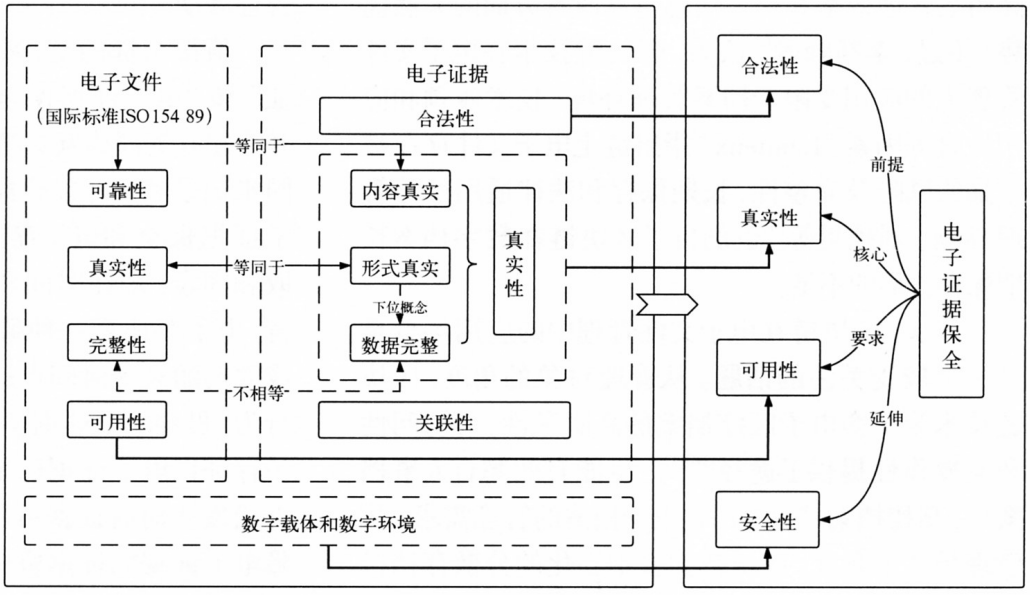

图1 电子证据保全的基本要素

系统，通过司法区块链、可信电子证据平台和司法信用共治平台实现电子证据的安全存储、传输和访问，以有效保全电子证据全生命周期的合法性、真实性、安全性和可用性，其电子证据保全模式如图2所示。

在合法性上，司法区块链中电子证据的合法性由国家法律赋予，广州互联网法院通过内部规范建设进一步具体化和操作化，并且推进证据规则和裁判经验的输出，将司法规则前置到外部主体的规则和平台建设中，构筑起信用生态系统的基石。

在真实性上，广州互联网法院通过区块链全程监管和多阶段哈希值校验的方式，确保链上电子证据不可篡改和留痕可溯，实现电子证据的形式真实，并采取多链聚合和多主体背书的策略构建去中心化的信任网络，维护电子证据的内容真实。

在安全性上，广州互联网法院利用哈希算法和非对称加密算法的数据保密优势对电子证据进行加密管理，以分布式存储理念打造电子证据的存储基地，并配套系统防护机制，确保电子证据的安全可控。

在可用性上，广州互联网法院一方面以清晰、合规的元数据方案满足对电子证据的检索需求，另一方面通过对结案电子证据的格式转换、脱机归档和定期检测确保电子证据的持续可用。

下文将围绕这一保全模式，以广州互联网法院的实践为分析对象，阐述如何借助制度、技术、管理和社会等多种因素的融合，实现电子证据在合法性、真实性、安全性和可用性等维度的保全。

4 广州互联网法院的电子证据保全策略分析

4.1 合法性保全策略

面对电子证据合法性保全需求，广州互联网法院以制度先行为原则，为电子证据的形成、固定、保管等环节提供可执行的标准规范，成为电子证据和互联网诉讼合法化和规范化的重要前提。

4.1.1 司法认可

最高人民法院《关于互联网法院审理案件若干问题的规定》(法释[2018]16号)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、

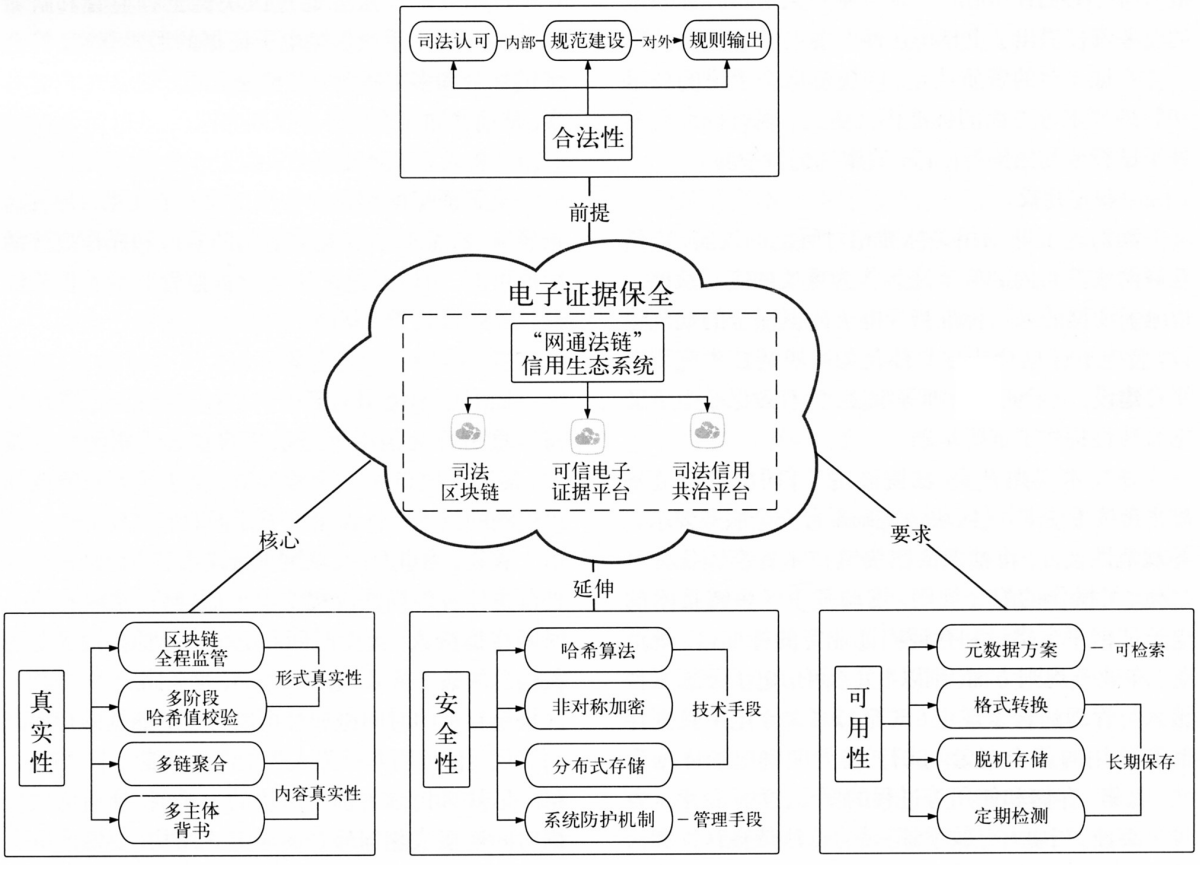

图2 基于区块链的电子证据保全模式

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，互联网法院应当确认。”《人民法院在线诉讼规则》(法释[2021]12号)也规定，“当事人作为证据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，人民法院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。”这些规定在司法层面上认可了区块链在电子证据保全中的作用，成为区块链上电子证据合法性的首要来源。

在技术应用标准上，司法部《电子数据存证技术规范》(SF/T 0076-2020)是国家层面关于区块链电子证据的最新司法鉴定技术规范。上海司法鉴定协会起草的《基于区块链技术的电子数据存证规范》(T/SHSFJD 0001-2020)则对区块链存证系统的业务流程提出了更具操作性的要求。不过，目前第三方存证平台的资质认定、区块链保全手段的技术和管理要求等方面的标准仍然匮乏，现有标准也多处于试行或初始施行阶段，适用性仍待检验。

4.1.2 规范建设

面对电子证据相关标准相对匮乏的现实，广州互联网法院将内部规范建设作为重要的应对策略，以电子证据的采信标准指导电子证据保全的规范建设，将电子证据合法性具体化为区块链技术应用、平台建设、电子证据管理等维度，为有效保全电子证据合法性提供了重要基础。

在技术规则方面，法院制定了《司法区块链基础平台技术要求》《区块链基础平台安全服务要求》等规范性文件，将抽象的区块链技术标准固化为可视化、可操作的配套规则，推动基于区块链技术的电子证据平台建设和存证固证业务的标准化、规范化。在业务规则方面，则以《关于可信电子证据平台接入与管理的若干规定(试行)》《关于电子数据存储和使用的若干规定(试行)》等明确电子证据生成、收集、存储和使用等过程的要求，为平台接入方规范存证、当事人有效举证、法官依法依规认证和法院电子证据管理业务提供了可参照的文本。

4.1.3 规则输出

目前，广州互联网法院信用生态系统中的电子证据有四大来源，即案件当事人、依法提供电子证据。存证服务的第三方存证平台、依法提供公证或鉴定服务的组织机构，以及依法获取和提供电子证据的互联网平台。证据来源多样化必然要面对不同主体间技术标准和存证规则不统一的问题。对此，法院依托内部规范建设的既有成果，向外输出证据规则和裁判经验，将司法规则前置到外部主体的规则和平台建设，帮助互联网企业和第三方存证平台明确业务数据保存范围或存证、固证标准，引导社会主体参照司法部门的示范性庭审案例进行服务和产品的合规化设计。

规则输出是解决多主体间业务规则相异和多来源电子证据统一性难题的创造性举措，是“前端控制”理念指导下保全电子证据合法性的前置性措施。通过向外部主体输出规则，可以从源头对电子证据进行规范和控制，确保外部主体提交的电子证据符合有效存证的技术标准、内容要求和格式规范，补强电子证据的合法性。

4.2 真实性保全策略

广州互联网法院通过区块链全程监管和哈希值校验的技术手段保障电子证据的形式真实，综合多链聚合和多主体背书策略强化电子证据的内容真实，从而共同保全电子证据真实性。

4.2.1 形式真实性的保全策略

电子证据的形式真实性指向电子证据自形成后未经篡改，意味着证据内容的防篡改和操作痕迹的留痕可溯，可以通过区块链全程监管和哈希值阶段性校验的方式予以保障。

4.2.1.1 区块链全程监管

面对电子证据易篡改的特征，广州互联网法院将区块链作为信用生态系统的基础规则和底层技术，借助区块链实施全程监管，基于其不可篡改和可追溯的技术特性保全电子证据的形式真实性。

首先，当事人、互联网平台或第三方存证平台等外部主体在线向法院提交电子证据后，法院在第一时间将提交人、提交时间和电子证据原始内容等相关信息的数字摘要值上链存储，永久固定。一方面，区块链自带的时间戳属性可以为电子证据的形成时间提供可信证明并排除人为干涉的可能。另一方面，每一区块都记录着前一区块的哈希值，所有区块

根据时间连接成相互环扣的块链式结构，要修改链上某一区块必须同时推翻该区块往后的所有区块；重新确认交易的过高算力成本意味着链上电子证据几乎不可能被篡改。

其次，法院将电子证据自上链到永久保存或销毁的整个生命周期置于区块链的监管下，利用区块链的可追溯特性实现全过程管理。司法区块链不仅存储电子证据等业务数据，还同步保存电子证据形成、流转、查询、应用等过程的痕迹数据，确保任何授权或非授权的数据访问、修改、加密或移除行为都透明可溯且不可抵赖。

4.2.1.2 多阶段哈希值校验

电子证据生成、传输、使用和存储的过程涉及多个参与主体，且数字化信息具有易变性和可操作性，因此有必要对电子证据进行数据认证和完整性校验。哈希值校验使用哈希算法将信息压缩映射为长度固定的数字摘要值，并对不同阶段计算输出的摘要值进行比对。哈希算法具有强抗碰撞性，同一明文的哈希值总是相同的，不同明文则很难有同样的哈希值，因此任何对原始信息的修改都必然导致哈希值的变化。

基于这一特性，广州互联网法院通过哈希值校验对电子证据完整性进行实时监测。在事先存证阶段，法院对所接收的电子证据进行哈希值计算并上传到外网区块链。诉讼发生时，电子证据的原始内容和数据哈希值将被一并传送到法院内网，通过哈希值校验后上传到内网区块链上永久存储。在取证质证阶段则根据存证编号获取链上的存证内容，并对司法区块链所返回的摘要值和存证时间等数据进行哈希值校验，完成对电子证据的完整性检测。

在电子证据生命周期的不同阶段进行数据哈希值校验，能够在经办人员身份复杂、数字信息易操作的背景下更好地应对电子证据的防篡改难题，规避对链上电子证据的非法操作，保证电子证据流转和存储过程中的形式真实性。

4.2.2 内容真实性的保全策略

区块链和哈希校验等技术手段能够保障链上电子证据的不可篡改和形式真实，却难以证明电子证据在上链存储前的内容真实。对此，多链聚合和多主体背书等社会化参与的策略，为电子证据的内容真实性保全提供了新思路。

4.2.2.1 多链聚合

在互联网诉讼中，电子证据的特性决定了当事人自主取证和举证的难度大且证据可采性低。对此，广州互联网法院突破传统的区块链节点管理和数据调取模式，提出了多链聚合的思路。广州互联网法院选取市中院、市知产法院、市铁路中院等八家政法单位作为关键节点，组建司法区块链，共享存证数据和诉讼审判数据。同时，法院对接三大运营商、金融机构、大型互联网企业和第三方司法服务平台等30多家单位，聚合企业自有链，构建可信电子证据平台，实现电子证据的规范存储和便捷调取。法院以“网通法链”信用生态系统为连接点，聚合司法区块链、企业自有链和社会合作链，破除接入主体间的数据壁垒，并建设统一的存证接口和标准化的服务接口，实现多方主体间的数据互联互通和可控流转。

当网络诉讼成立时，当事人可以通过“一链两平台”对第三方存证平台、互联网企业等接入方事先存储的数据进行自动调取，并直接作为诉讼证据使用。一旦多份电子证据的内容具有协调性和一致性，且证据之间能够通过相互印证和有序衔接构成完整的证据链闭环，排除对案件事实的合理怀疑，就可以认为这些涉诉电子证据能够充分、准确地反映客观的案件事实，可以予以信任和采用。

在多链聚合的模式下，法院有效确保了网络诉讼中充足的可信电子证据来源，在此基础上借助证据链闭环机制，便能在一定程度上实现对电子证据内容真实性的验证。

4.2.2.2 多主体背书

在传统的信任模式下，电子证据的内容真实性一般依靠网络公证处的公证书或时间戳服务中心签发的可信时间戳凭证加以保全和证明，其实质仍是一种依托权威机构公信力进行背书的中心化信任逻辑，具有对公共权力的强依赖性。基于区块链的电子证据真实性保全策略则借鉴去中心化信任模式，以区块链的自我背书能力为依托，通过多主体共同背书的信任网络实现。

首先，广州互联网法院通过信用生态系统实现

与互联网企业、金融机构、第三方司法服务平台等主体的数据共享。从证据来源的角度，接入主体并非网络诉讼的直接利益相关者，而是相对中立的数据提供方，不具有伪造、篡改证据的足够动机。从验证机制的角度，法院并非采取单一主体或单份证据自我证明的真实性认证手段，而是通过多方主体提供的多份证据间的相互印证构成证据链。单一主体容易伪造或篡改掌握的电子证据，但在多主体共同背书的信任网络中，虚假证据必然与其他证据产生矛盾和冲突，从而丧失证据资格。

其次，法院通过“一链两平台”确保信任网络中的数据对接和同步，除特殊权限规定外，网络中的电子证据摘要值和对电子证据的操作记录同时对整个网络中的所有节点公开。信任网络中的广州互联网法院接受上级法院、检察院等司法主体的协同监督，又联合仲裁、公证、互联网企业、第三方存证平台等外部主体建立社会监督机制，通过多方监督和共同背书强化电子证据的可靠性。

多主体共同背书的管理模式借助多元主体的协同实现对电子证据的共同维护、治理和监督，规避了单一中心控制下电子证据的信任风险，为保全电子证据的内容真实提供了去中心化的信任网络。

4.3 安全性保全策略

面对网络攻击、非法入侵和软硬件受损等隐患带来的数据外泄和丢失风险，电子证据保全需要通过加密存储、保密传输和分布式存储等手段确保传输、存储和使用过程中的安全可控。

4.3.1 哈希算法加密存储

哈希算法是基于哈希函数的密码学方法，常用于对不适合公开的数据进行保密处理。广州互联网法院以“只存摘要值，不存原始数据”为原则，利用哈希算法对电子证据进行加密存储。对于事先存证的电子证据，法院通过哈希算法输出其摘要值并上链存储，仅当诉讼发生时才调取涉诉电子证据原文。哈希函数作为单向转换的散列函数，具有不可逆性。一旦发生恶意攻击或系统入侵等极端情况，窃取者仅能获取到电子证据的摘要值，无法据此逆推出其所指向的电子证据的原始内容。基于哈希算法的加密式存储措施有效回应了电子证据高保密性的需求，确保了电子证据的存储安全。

4.3.2 非对称加密算法保密传输

面对内外网电子证据的摆渡需求，利用非对称加密算法对电子证据进行保密式传输是容易实现且成本较低的策略。具体方式为事前生成一对公钥和私钥，公钥公开，任何人均可使用公钥加密信息，但只有私钥能解密信息。在进行电子证据传输时，利用公钥加密外网区块链上的电子证据及证据摘要值后，将密文传入法院内网后，仅有法院可以使用内部保管的私钥进行解密并获取原始数据内容。在这一过程中，非对称加密算法利用公、私密钥分别实现了发送者身份校验和数据安全保密目的，确保了内外区块链间电子证据的传输安全。

传统的电子证据管理多采用集中式存储模式和数据备份的安全管理模式，分布式存储则为强化电子证据的安全防护能力提供了新思路。

4.3.3 分布式存储

分布式存储模式将数据分散在虚拟网络中的多个节点而非寄存于一个中心服务器，汇集全网节点的算力更新、记录、存储和维护数据，保障系统的持续稳定和数据安全。广州互联网法院遵循分布式存储思路，构建私有云存储基地并配备“两地三中心”数据容灾方案，推动电子证据的安全管理转向系统维稳和数据灾备协同。

在系统维稳方面，法院构建了基于私有云的基础运行环境。云存储具有分布式和去中心化特征，云上电子证据通过数量庞大的节点进行相互验证和共同维护，除非同时控制网络中51%以上的节点，修改单个节点上的数据都是无效的。当系统中某个节点受到恶意攻击或单台物理机出现硬件故障时，其他节点仍能继续发挥作用。各节点的数据互为备份，有效规避了网络崩溃引起的服务中断或数据丢失、受损等不可逆的灾难性后果，降低了电子证据的安全风险。

在数据容灾方面，法院采用“两地三中心”灾备模式。为了强化数据瞬时恢复能力，法院一方面在同城建立一个与自身具备同等数据处理能力的灾备中心，通过数据同步复制实现电子证据的实时在线更新和备份，满足灾难情况下的应急切换需求；另一

方面在异地建立独立的灾备中心，与同城双中心保持定期异步复制，实现增量数据备份，并在同城双中心发生故障时减少数据丢失和受损，承担起业务恢复功能。“两地三中心”是极具应用性的数据灾备模式，能够有效维护业务过程中的数据稳定性和办结归档电子证据的安全性。

4.3.4 建立系统防护机制

为了规避系统漏洞和非法访问带来的安全风险，需要从系统设计到运行层面配套相应的管理机制，实现电子证据的自主可控和机密安全。

在系统设计层面，广州互联网法院联合工信部五所共同起草区块链技术标准，并委托国内大型互联网企业对司法区块链进行定制化开发和安全部署，基于国产化软硬件资源构建电子证据管理系统和底层环境。同时，法院配备了具备区块链应用和管理能力的内部技术团队，实现系统的独立运维和自主控制。另外，法院为内部网络设置了第三级安全等级，较一般要求高出一个等级，以阻隔网络攻击和系统入侵。

在系统运行层面，法院通过多节点授权机制实现访问控制，规避盗窃风险，保障电子证据使用过程中的数据安全。通过合理的节点设计，法院为相关主体分配对应的电子证据查询和使用权限。在诉讼过程中，经办法官、案件当事人等相关主体通过实名和活体认证后，均可对权限范围内的电子证据和案件信息进行联网、远程、跨院查询与办理。同时，案件材料一经查看，就会自动加盖操作者的身份水印，以此实现违规操作行为的不可抵赖。权限管理措施在保障数据联通和无缝流转的同时，有效防止了非授权访问造成的电子证据泄露和隐私侵害风险。

4.4 可用性保全策略

为确保电子证据在长期保存过程中保持可被查询和检索，可以持续存取、识别和理解的状态，需要将可用性纳入电子证据保全的范围，从电子证据现行阶段到归档保存阶段予以连续性保障。

首先，通过构建高质量的元数据管理体系满足电子证据检索需求。根据国家规范和上级法院要求，广州互联网法院对电子证据的元数据要素进行梳理，初步形成一套元数据方案并配置到业务系统。业务系统依据事先配置的规则，对案件过程中持续累积的电子证据进行元数据信息的自动抽取并随案同步归档。为了兼顾数据检索和信息保密需求，链上仅存储检索元数据信息和电子证据摘要值，各级节点通过相关的结构化数据对电子证据进行快速检索，必要时申请查调相应的原始内容。

其次，针对电子证据可识别、可理解需求，则以格式转换、脱机存储和定期检测为对策。一方面，法院选取常规的可用格式对电子证据存储格式进行必要转换，确保一般的系统升级不对其读取和识别造成影响。另一方面，根据诉讼档案归档办法和保管期限规定，法院选取相应的脱机存储介质，将已办结的电子证据及其元数据、背景信息和软硬件环境等一并刻录归档；同时通过定期抽检与全检，对不符合检测要求的电子证据进行及时的数据恢复，确保电子证据的持续可用。

5 结论与展望

如上所述，为了有效回应网络诉讼对电子证据提出的新诉求，广州互联网法院构建了“网通法链”信用生态系统，为电子证据的可采、可信、可控和可用管理配套系统的电子证据保全措施。

针对电子证据易篡改、易伪造、易消亡等特性，广州互联网法院借助司法认可、规范建设和规则输出保障电子证据合法性；通过区块链全程监管、多阶段哈希值校验等方式和多链聚合、多主体背书的策略维护电子证据的真实性；以哈希算法、非对称加密、分布式存储和系统防护机制确保电子证据的安全可控；通过元数据抽取、格式转换、数据脱机存储和定期检测维护电子证据可用性。在融合制度、技术、管理和社会等多种因素的基础上，广州互联网法院构建起综合的电子证据保全系统，有效支撑了电子证据的合法性、真实性、安全性和可用性保全需求。

不过，广州互联网法院电子证据保全策略作为对区块链的创新应用模式，仍处于初步探索阶段，在理论和实践上依然面临着相应挑战。

首先，就区块链的应用而言，一方面，事先存证使得节点存储的数据体量不断增大，产生大量冗余数据，导致司法区块链的存储和计算负担持续加重，在一定程度上拉低了区块链的运行性能；另一

方面，区块链本身并不适合频繁的数据输出和信息交互，与电子证据快速存取的需求形成矛盾。对此，法院需要重新划分业务边界，探索存证和取证相分离的发展思路，将存证业务转移到第三方司法服务机构上，并通过规则输出指导第三方机构规范存证，在保障电子证据存取效率的同时兼顾电子证据的质量要求。

其次，就可用性而言，确保电子证据的可用性意味着“确定所有电子证据的保管期限是否应当长于当前存储系统的寿命”，但长期保存仍是区块链技术成功应用需要解决的关键问题[33]，区块链的技术寿命也同样值得关注。对此，美国国家档案与文件署(NARA)在《电子文件管理通用要求》提出的“制订在当前系统淘汰前将电子证据迁移到新系统的规划”“确保在云服务商终止服务时电子文件的迁移和存储”等都是值得借鉴的统筹性规划。

需要指出的是，虽然本研究以广州互联网法院为例，探讨了基于区块链的电子证据保全模式，但是司法机构和第三方存证平台等主体的电子证据保全实践仍在不断深化和发展。理论层面只有对此保持关注和持续跟进，与实践形成良好互动，并通过进一步的理论思考和归纳研究构建起系统的电子证据保全框架，才能有效应对技术发展和现实需求对电子证据保全带来的影响和冲击。

参考文献：

[1][25]祁天娇.基于电子文件管理视角的互联网电子证据保全研究[J].档案与建设，2018(3)：8-11，35.

[2]余亚荣，张照余.基于公证保全模式的电子文件法律证据价值维护研究[J].档案学研究，2020(4)：110-114.

[3]余亚荣，张照余.基于可信时间戳服务的电子档案证据取证和验证方案设计[J].档案管理，2020(1)：66-68.

[4][8]Lemieux V L. Blockchain recordkeeping: a SWOT analysis[J]. Information Management, 2017(6): 20-27.

[5]Findlay C. Participatory cultures, trust technologies and decentralisation: innovation opportunities for recordkeeping[J]. Archives & Manuscripts, 2017, 45(3): 176-190.

[6]刘越男.区块链技术在文件档案管理中的应用初探[J].浙江档案，2018(5)：7-11.

[7]李高峰，马国胜，胡国强.现阶段区块链技术在档案管理中不可行分析[J].档案管理，2018(5)：30-32.

[9][33]刘越男，吴云鹏.基于区块链的数字档案长期保存：既有探索及未来发展[J].档案学通讯，2018(6)：44-53.

[10]Dagher G G, Mohler J, Milojkovic M, et al. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology[J]. Sustainable Cities and Society, 2018, 39: 283-297.

[11]Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications[J]. Journal of Information Security and Applications, 2020, 50(Feb.): 102407.1-102407.13.

[12]孙大东，张文宁.人事电子档案安全管理区块链技术应用研究[J].档案与建设，2018(9)：26-29.

[13]张倩.区块链技术对高校档案信息管理方式创新的可行性探究[J].档案与建设，2017(12)：21-24.

[14]Findlay C. Decentralised and inviolate: the blockchain and its uses for digital archives[EB/OL].[2020-02-19]. https://rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses-for-digital-archives/.

[15]孙大东，杨晗.电子档案单套制管理区块链模式应用研究[J].浙江档案，2018(9)：7-9.

[16]蔡盈芳.电子档案管理应用区块链存储方式探析[J].档案学研究，2020(4)：104-109.

[17]潘虹，王子鹏.区块链技术对社交媒体信息归档的应用 探究[J].中国档案，2018(6)：74-77.

[18]马仁杰，沙洲.基于联盟区块链的档案信息资源共享模式研究——以长三角地区为例[J].档案学研究，2019(1)：61-68.

[19]刘庆悦.基于区块链技术的电子档案管理模型探析[J].浙江档案，2018(10)：22-24.

[20]王平，李沐妍，刘晓春.区块链视角下文件档案管理可信生态的构建[J].档案学研究，2020(4)：115-121.

[21]Bell M, Green A, Sheridan J, Collomosse J, et al. Underscoring archival authenticity with blockchain technology[J]. Insights: The UKSG Journal, 2019(1): 21.

[22]Lemieux V L. Trusting records: is Blockchain technology the answer?[J]. Records Management Journal, 2016(2): 110-139.

[23]Galiev A, Prokopyev N, Ishmukhametov S, et al. Archain: a novel blockchain based archival system[A]. IEEE. 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability(WorldS4)[C]. London: IEEE, 2018: 84-89.

[24][31]许海涛.区块链技术在可信电子文件管理中的适用性研究[J].山西档案，2019(6)：1-9.

[26]毕玉谦.民事诉讼电子数据证据规则研究[M].北京：中国政法大学出版社，2016：5-6，382-383.

[27][28][29][30]王燃.电子文件管理与证据法规则的契合研究[J].档案学通讯，2018(5)：51-56.

[32][英]丹尼尔·德雷舍.区块链基础知25讲[M].马丹，王扶桑，张初阳，译.北京：人民邮电出版社，2018：27.