区块链赋能档案信息安全管理实践研究

文 | 钟海琪

随着数字化进程快速且迅猛地发展，档案信息安全管理工作正面临存储漏洞、权限混乱以及追溯困难等严峻挑战，现有的管理方式已难以有效应对当前形势。区块链技术的出现为档案信息安全防护提供了全新的解决思路，其分布式账本、智能合约等核心机制与档案安全管理需求高度契合，深入探讨区块链赋能档案信息安全管理具有重要现实意义。

（配图由 AI 生成）

区块链赋能档案信息安全管理的理论基础

区块链技术的蓬勃发展为档案信息管理工作带来全新理论支持与变革动力，深入剖析区块链技术与档案信息管理之间的内在逻辑和紧密联系，是有效推动档案管理领域实现创新赋能的关键前提与重要基础。

区块链技术与档案安全管理的内在契合

档案信息安全管理的根本要求是保证档案信息真实、流转过程可控以及责任归属可追溯。区块链的去中心化账本技术规避了传统集中存储模式下单点故障问题，数据写入区块链后就无法被篡改，为保护档案真实性提供了坚实技术基础。智能合约的自动执行功能强化了权限管理刚性，让授权行为从主观判断变为规则驱动的客观过程，从而减少了人为操作引发的管理风险。哈希算法和时间戳技术协同作用，为档案从创建到销毁全过程构建了可信审计轨迹，确保每一步操作都可验证且不可抵赖。这两者在安全目标、管理机制和实现方法上高度契合，为区块链技术在档案安全管理领域的应用提供可靠理论支撑。

区块链赋能档案安全管理的理论框架

区块链赋能档案安全管理的理论框架涵盖技术支撑、管理优化和制度协同三个维度。在技术层面上，分布式存储、非对称加密以及共识机制共同构成档案安全保障的基础体系，分别通过数据存储、身份验证和多方协作构建起全方位防护屏障。在管理层面，区块链把传统人工审核的权限控制机制转变为程序化自动执行流程，有效降低管理成本和操作失误风险，同时完整留存链上操作记录，为异常行为监测提供客观数据支撑。在制度层面，链上数据的可追溯性和公开透明特性为档案监管工作提供可验证的执行依据，推动档案管理模式从经验导向逐步转向证据导向。这三个维度相互依存且有机结合，共同构建起区块链技术赋能档案安全管理的完整理论体系。

档案信息安全管理的现实困境

在数字化进程不断推动的情况下，档案信息安全管理面临诸多潜在问题，存储方面存在的隐患、权限管理的混乱以及追溯困难等多种因素相互交织，严重阻碍了档案管理的现代化发展进程。

档案存储与传输环节的安全隐患

数字档案的大规模集中存储在提升管理效率的同时，也集聚了相当程度的安全风险。集中式存储架构天然存在单点故障隐患，一旦遭遇外部攻击或系统崩溃，海量档案数据将面临不可逆的损毁乃至永久性丢失。在传输环节，档案数据流转于各节点之间，网络截获、中间人攻击、数据篡改等威胁始终潜伏其中，加之部分档案管理机构的网络安全防护能力参差不齐，薄弱环节极易成为攻击突破口。现有备份机制往往流于形式，容灾预案的制定与实际执行之间存在明显落差，定期演练缺失导致应急响应能力严重不足。档案数据的完整性长期处于脆弱状态，安全隐患贯穿存储与传输的全过程，潜在损失难以估量。

档案访问权限管控的失序风险

在档案信息安全管理中，权限管控的无序状态是极具隐蔽性且破坏力大的核心难题。当前主流权限管控体系大多采用固定不变授权模式，这种静态机制难以适应档案应用场景的多样需求，导致权限边界模糊且越界访问行为频发。内部人员违规操作的风险特别严峻，个别档案工作者利用职务

之便私自查阅、篡改，甚至销毁机密档案，既有的审计流程通常在违规行为发生后才启动，给事后的追责工作造成巨大障碍。对于外部访问的控制同样存在显著缺陷，身份验证体系不完善，使未获授权者伪造身份信息非法侵入档案系统情况时有发生，更严峻的是跨机构档案资料共享过程中权限协同管理几乎空白，数据在不同主体间的流动界限难以界定。权限管控的整体混乱深刻揭示了档案安全管理工作在制度规范与技术保障层面均有明显不足。

档案真实性认定与责任追溯的缺失

档案的真实性是其具备证明效力的核心基础，可当前管理体系在确保真实性方面有显著不足。电子档案本身有易于修改的特性，使得档案原始状态难以准确核实，判断是否被恶意篡改，往往缺乏有力技术支撑，现有的电子签名技术不管在应用范围还是实施深度上，都无法充分满足保障档案安全的实际需求。档案操作过程中的记录保存机制普遍存在短板，各环节操作人员的具体行为难以完整留存与固定，若发生档案遗失或数据外泄等情况，追责会因缺乏必要证据而陷入困境。追溯链条的断裂不仅削弱档案管理的约束力，还使问责体系流于形式，有些单位以技术能力不足为借口推卸责任，极大损害社会大众对档案资料可信度的信任基础。

区块链赋能档案信息安全管理的实践路径

对理论逻辑进行梳理以及呈现现实存在的矛盾，二者共同揭示出区块链技术应用于档案安全管理的发展路径，其核心要点在于如何将技术优势转化为具备可操作性与长期稳定性的管理能力。

区块链赋能档案安全管理的具体运用

将区块链技术应用到档案安全管理中，其核心功能主要体现在存储安全、权限控制与操作记录三个方面。在存储方面，档案数据哈希值上链之后，任何微小改动都会使哈希值发生变化，这既保证了档案原始性以防止内外部篡改，又通过分布式节点冗余存储避免单点故障造成的数据丢失问题。在权限管理方面，智能合约能够自动执行授权和撤权操作，同时会将档案调阅、修改、移交等操作记录在链上，彻底解决传统人工审批模式下权限管理松散的问题。在全程留痕方面，区块链的时序性账本自然契合档案全生命周期管理需求，从档案形成到归档、利用再到销毁，每个环节的操作都被固定在链上，便于快速定位和追溯异常行为，以构建完整的数字信任链条。

区块链赋能档案安全的推进策略

档案安全管理通过区块链技术实现革新是个系统性工程，需要分阶段有策略地有序落实，起步阶段建议优先挑选业务流程相对独立、数据保密性要求较高的档案类别开展小范围试验。在限定条件下逐步掌握技术实施方案，为后续全面铺开奠定基础并规避可能的实施障碍。在技术架构层面，联盟链凭借能保障数据交互又能实施权限控制的特性，更贴合档案管理部门的现实工作场景。和完全开放的公有链架构相比，在保障信息机密性与提升运行效能方面达成了更合理的折中，实施过程中应着重解决档案管理系统与区块链平台间的对接标准化问题，从项目规划初期就需统筹设计数据流通机制，防止出现新的信息壁垒。技术升级和人员培训需要双管齐下，档案工作者对区块链技术原理的掌握程度直接关系到最终应用成效，若仅侧重技术部署而忽略人员适配，很可能导致应用停留在形式层面而无法释放实际价值。

区块链赋能档案安全的保障体系构建

技术落地得依靠完善的保障体系来支撑，制度、标准和人才这三个环节缺一不可。在制度层面，当下档案法规对于区块链存证的法律效力还没给出清晰说明，亟须完善相关立法或者制定专项政策，以此确保链上档案数据具备完整的法律凭证效力，并且构建链上数据管理责任追责机制，让制度约束和技术手段协同发挥作用。在标准方面，区块链档案管理所涉及的数据格式、上链流程、节点准入以及隐私保护等技术标准较为零散，统一的行业规范是实现跨机构档案数据互通共享的根本前提，标准不足会使得各地实践难以形成有效协同。在人才方面，复合型档案管理人才短缺是限制赋能深度的关键因素，培养既掌握档案专业知识又理解区块链技术的专业团队，要把高校培养、在职培训和实践锻炼三者结合起来，建立科学的人才梯队，为区块链在档案安全管理领域的深度应用提供最核心的智力保障。

结束语

区块链技术能给档案信息安全管理提供可信存储、精确权限控制以及全过程追溯技术保障，从根本上解决传统管理方式长期存在的诸多难题。推动区块链技术应用到档案安全管理是一项复杂的系统性工作，要在完善理论指导下，结合档案管理实际问题制定合理计划并分阶段实施部署，同时，完善技术、制度、人才等方面配套保障机制，持续提升档案信息管理安全能力与整体水平，为数字档案行业长远发展筑牢更稳固基础。

作者简介：钟海琪　深圳地质建设工程公司

责任编辑：孙姗姗　**投稿邮箱：**zhouhl@staff.ccidnet.com