 DOI: https://doi.org/10.12345/daglyqyfzyj.v4i3.37807

Research on Blockchain Technology Applications in Secure Electronic Archives Management

Jinquan Tong

People's Government of Huerle Town, Zhalait Banner, Xing' an League, Inner Mongolia, 137617, China

Abstract

As critical information assets, electronic archives' authenticity, integrity, and traceability play pivotal roles in administrative governance and social governance. Traditional centralized storage models face challenges including high tampering risks, opaque auditing processes, and system vulnerabilities. Blockchain-based solutions—such as hash verification, consensus mechanisms, smart contracts, and distributed storage—can establish a comprehensive security framework covering evidence preservation, tamper-proofing, sharing, and long-term archiving. By embedding on-chain verification and automated rule enforcement throughout the entire lifecycle of archives (from creation to utilization), the credibility and circulation security of electronic archives are significantly enhanced, facilitating the transition from centralized trust to technology-driven trust in management models.

Keywords

Blockchain technology; Electronic records; Information security

区块链技术在电子档案安全保管中的应用研究

佟金权

内蒙古自治区兴安盟扎赉特旗胡尔勒镇人民政府，中国·内蒙古 兴安盟 137617

摘　要

电子档案作为重要的信息资产，其真实性、完整性与可追溯性对行政管理和社会治理具有关键影响。传统集中式存储模式存在篡改风险高、审计不透明和系统脆弱性强等问题。基于区块链的哈希上链、共识机制、智能合约与分布式存储，可构建覆盖存证、防篡改、共享与长期保存的安全体系。通过在档案生成、管理与利用全流程嵌入链上验证与自动化规则执行，电子档案的可信度和流转安全性得到显著提升，促进管理模式从中心化信任向技术信任转型。

关键词

区块链技术；电子档案；信息安全

1 引言

在政府、企事业单位信息化快速发展的背景下，电子档案已逐渐取代纸质档案，成为记录行政行为与社会活动的重要凭证。然而，传统电子档案保管方式存在显著弊端：中心化存储容易遭受黑客攻击，数据在传输或迁移中存在被篡改的风险，档案真实性难以保障；同时，缺乏统一的信任机制和跨系统数据互认标准，导致档案共享受限，管理成本上升。区块链技术以其独特的分布式结构和密码学安全机制，为电子档案的全生命周期管理提供了新思路。通过时间戳、哈希函数、智能合约与共识算法等机制，区块链能够实现档案数据的确权、防伪与可信共享。本文从技术架构与应用层面系统分析区块链技术在电子档案安全保管中的作用与实践路径，旨在推动档案信息安全体系的创新发展，实现档案管理的透明化、智能化与可信化。

【作者简介】佟金权（1972—），男，蒙古族，中国内蒙古兴安盟扎赉特旗人，本科，档案馆员，从事档案管理研究。

2 区块链技术的原理与电子档案安全需求分析

2.1 区块链技术的基本原理与特征

区块链技术是一种基于密码学和分布式网络的去中心化数据库系统，其核心结构由数据区块和链式链接组成。每个区块包含时间戳、交易数据和哈希摘要，后一区块通过记录前一区块的哈希值，形成不可篡改的链式结构。区块链的关键特征包括去中心化存储、不可篡改性、可追溯性和智能合约。去中心化存储使得数据分布在多个节点上，避免了单点故障的风险；不可篡改性确保了任何数据修改都会被全网节点记录和验证，保障数据的真实性；可追溯性使得每条数据都可以追溯到原始来源，并具有时间戳和历史记录；智能合约则能够根据预设规则自动执行合同内容，减少人为干预[1]。这些特征与电子档案管理对真实性、完整性、安全性和可追溯性的要求高度契合，为档案管理体系的重构提供了强有力的技术基础。

2.2 电子档案安全保管的核心要求

电子档案的安全保管涉及档案数据的防篡改、信息泄漏保护以及档案的全生命周期管理。其核心要求包括：真实性、完整性、可追溯性和持久性。真实性要求确保档案在生成、传输和存储过程中未被篡改，保持数据的原始性；完整性则指保证档案数据及元数据在存储和传输过程中不被损坏或丢失；可追溯性要求能够记录档案从生成到销毁的全过程，并确保每一步操作都有清晰的记录；持久性则是确保档案在长期保存过程中能够被读取和验证。在传统的电子档案管理中，这些要求依赖于集中式数据库和人工审核，存在系统漏洞、操作错误以及数据迁移等潜在风险，容易受到人为因素的影响。

2.3 区块链赋能电子档案安全的契合性分析

区块链技术的哈希加密和分布式账本机制能够保证电子档案在存储、传输和操作过程中的数据安全。每次档案操作都会被全网节点验证并记录，从而形成永久的操作记录。区块链的去中心化特性消除了传统模式中的“信任中介”，有效避免了数据在传输和存储过程中的篡改问题。此外，通过智能合约，可以实现档案访问控制、权限验证和自动审计，确保档案的管理过程更加透明和安全。智能合约能够自动执行预设的规则，避免人工干预带来的风险，提升操作效率和合规性。区块链技术的引入，促进了从“中心信任”到“技术信任”的转变，为电子档案建立了一个可信的生态系统。

3 区块链技术在电子档案管理中的应用架构

3.1 区块链 + 电子档案系统总体结构

基于区块链的电子档案系统主要由“数据层—网络层—共识层—合约层—应用层”五个部分构成，每一层在系统的整体架构中扮演着重要角色。数据层主要负责存储档案的哈希摘要与元数据，确保档案的完整性和不可篡改性；网络层则通过节点之间的通信与数据广播实现系统的去中心化，确保信息在各节点间的流通与共享；共识层采用如 PoW（工作量证明）、PoS（权益证明）、PBFT（拜占庭容错协议）等算法，确保全网数据一致性与安全性；合约层部署访问控制与档案操作规则，确保对档案的访问与操作符合预定的规范；应用层提供档案查询、验证、共享与统计分析功能，为用户提供便捷的操作界面和强大的数据处理能力。在该架构中，档案原文件可采用链下分布式存储技术（如 IPFS），而哈希值和索引信息上链，从而既保障数据的安全性，又提高了系统的存储效率。

3.2 档案数据上链与身份认证机制

电子档案的上链过程包括档案数据摘要生成、加密签名与时间戳写入三个关键步骤[2]。首先，通过哈希算法（如 SHA-256）计算档案的指纹，生成唯一的档案摘要；然后，利用数字签名对摘要进行加密，确保档案来源的可信性；最后，时间戳服务保证档案生成的唯一性与时间可验证性，确保档案在指定时间点的真实性。用户身份管理方面，系统可结合公钥基础设施（PKI）与区块链账户体系，实现多级权限控制。通过这种身份认证机制，只有经过授权的人员才能访问或修改档案内容，有效防止非法操作与越权访问，从而增强档案管理的安全性和可信度。

3.3 智能合约与档案操作自动化

智能合约在区块链电子档案系统中扮演着核心角色，能够通过预设的可编程脚本自动执行档案的操作。智能合约在档案生命周期管理中尤为重要，能够根据预定的规则自动触发和执行各种操作。例如，当档案达到保存期限、使用权限发生变化或审查周期到期时，智能合约可以自动执行档案的归档、转移或销毁等任务，并将这些操作的记录写入区块链账本中。通过这种方式，智能合约减少了人工干预，提高了工作效率和系统的安全性。同时，这一机制为审计与监管提供了数据支撑，使得档案操作的每个环节都能够透明可追溯，为合规性和透明度提供保障。

4 区块链技术保障电子档案安全的关键机制

4.1 防篡改与真实性保障机制

区块链技术的加密算法和链式结构使得档案数据的篡改变得几乎不可能。每个区块通过哈希值与前一个区块相连接，形成链式结构。一旦档案数据被写入区块，数据的哈希值就被固定下来，任何后续的修改都必须得到全网节点的一致确认才能进行[3]。这意味着，即使黑客成功攻破某一节点，也无法改变全网中已经存在的档案数据。此外，区块链的溯源机制能够全面记录档案的生成、访问和修改历史，确保档案数据的原始性和真实性。通过这种机制，不仅可以有效防止数据篡改，还能提供数据来源的可信依据，为档案的真实性验证提供强有力的技术支持。

4.2 分布式存储与数据冗余保障

与传统的集中式存储方式相比，区块链的分布式存储架构显著提高了数据的安全性与可靠性。在区块链网络中，档案数据被分布到多个节点上，且每个节点都保存一份数据副本。这种分布式存储方式能够有效避免单点故障的风险，即使部分节点损坏或失效，系统仍能保证数据的完整性和持续可用性。此外，结合分布式文件系统如 IPFS（InterPlanetary File System）或 HDFS（Hadoop Distributed File System），可以实现链上哈希与链下原文件的协同保护。这样，数据不仅在区块链上有哈希值的验证，也通过分布式文件系统存储原始文件，形成“链存证、链下存储”的安全模型，进一步提升档案数据的持久性和灾备能力。

4.3 可追溯与可验证审计机制

区块链提供的交易日志和时间戳记录，构成了电子档案的行为链。每一笔档案的访问、修改、转移等操作都会被完整记录在区块链中，形成一条不可篡改的“档案行为证据链”。这种记录机制为审计和监督提供了全面的保障。

审计机构可通过区块浏览器，实时查询档案的流转路径，迅速定位操作人、操作时间及其具体行为类型，确保档案操作的透明性与可追溯性。这种基于区块链技术的可追溯与可验证审计机制在司法取证、行政审查以及历史研究等领域具有重要意义，为确保档案管理的合规性和可靠性提供了有力的支持。

5 区块链电子档案安全保管的实践与发展策略

5.1 系统建设与技术优化路径

为实现区块链电子档案系统的落地，应构建一个融合“区块链 + 云平台 + 分布式存储”的综合架构。区块链技术能够为档案数据提供确权与安全验证，确保档案内容的真实性与完整性；云平台则为系统提供强大的计算和服务能力，支持数据的高效处理与管理；分布式存储则解决了文件存储的可扩展性和容灾能力问题。通过这种架构，可以在不同的存储节点之间实现数据的分布式管理，提高系统的容错性和扩展性。

跨链技术的引入能够有效打破信息孤岛，实现不同档案系统间的数据互联互认。政府、企事业单位等不同机构之间的档案数据可通过跨链实现无缝对接，提升信息共享和流通的效率。在技术优化方面，采用高效的共识算法是提高系统处理能力的关键。联盟链采用的 PBFT（Practical Byzantine Fault Tolerance）或 PoA（Proof of Authority）机制，能够在保证数据安全的前提下，提高系统的处理效率，特别是在政务档案的高并发需求下，能够实现快速响应与数据处理。

5.2 标准化体系与制度保障建设

电子档案区块链应用的发展离不开完善的标准化体系与制度保障。首先，必须建立国家级的电子档案区块链存证标准，明确技术规范，涵盖哈希算法的类型、数据上链的格式、节点的安全要求等方面。通过统一的标准，可以确保不同系统之间的互操作性与兼容性，避免因技术差异导致的信息孤岛和数据孤立问题。此外，国家标准还应明确区块链在档案管理中的应用范围，确保其在法律框架内运行。

为了实现区块链技术与现行档案法规的有效对接，必须进一步完善档案电子签章、身份认证、智能合约合法性等方面的标准和规范。电子签章是确保档案身份验证和数据不可篡改的重要保障，必须符合国家关于数字签名的法律法规；智能合约则要确保其在档案管理中的合规性，能够合法地自动执行合同条款，避免人为干预或误操作。最终，构建起“技术标准 + 安全规范 + 法律制度”三位一体的保障体系，为区块链技术在档案管理中的应用奠定基础，推动其规范化、系统化发展。

5.3 多链融合与隐私保护机制

在跨部门、跨区域的档案流转过程中，采用多链协同机制能够有效解决数据共享与安全隔离的矛盾。不同的档案类型和处理需求决定了不同的区块链技术应用场景。联盟链适合政府、企业与公众之间的档案共享与互动，能够实现分级访问和管理；私有链则适用于政府或企业内部对敏感档案的管理，确保档案数据的高安全性和保密性；公有链则适合用于公开的社会档案信息的存储与查询，保障公众对档案信息的访问。

隐私保护是区块链在电子档案管理中应用的另一大关键问题。通过采用先进的密码学技术，如零知识证明和同态加密，可以有效保护档案内容的隐私性。零知识证明技术能够在不泄露数据内容的情况下，验证档案的有效性与真实性，从而在确保数据安全的同时，满足法律和合规要求。另一方面，同态加密则可以让数据在加密状态下进行计算和验证，避免数据泄露或被篡改的风险。结合这两种技术，可以在实现档案信息安全管理的同时，保障档案的隐私性，推动区块链技术在档案管理领域的广泛应用。

6 结语

区块链技术的引入，为电子档案安全保管提供了全新的技术路径与治理模式。其不可篡改、分布式存储与智能合约等特性，使档案数据在形成、传输、存储与使用全过程中实现了“技术可信”的安全保障。基于区块链的电子档案管理体系，能够有效解决传统集中式系统的信任与安全瓶颈，推动档案工作从“管理驱动”向“信任驱动”转型。未来，随着人工智能、云计算与大数据分析的深度融合，区块链档案管理将实现智能化决策与全生命周期监管。各级档案机构应加强标准建设与跨链协作，形成安全、开放、可持续的电子档案生态系统，使档案成为社会信任体系的重要支撑与国家数字资产的重要组成部分。

参考文献

[1] 于宏艳.基于区块链技术的电子档案安全保护策略探讨[J].兰台世界,2024,(11):110-112.

[2] 冯姣.论区块链技术在电子档案保管中的适用及限度[J].档案学研究,2023,(05):131-139.

[3] 徐成俊,基于区块链技术的电子档案管理系统.甘肃省,兰州文理学院,2022-12-27.