CRYSTALIZING EMERGING TECHNOLOGIES, TRENDS AND PERSPECTIVES IN LIBRARIANSHIP:

A BOOK OF READING IN HONOUR OF

PROFESSOR NSE EMMANUEL AKWANG



EDITED BY:
PROF. AMANZE O. UNAGHA
PROF. CHINYERE A. OKEZIE
DR. KAYODE G. OYENIRAN
DR. COLUMBUS O. UDOFOT

First Published 2026

National Library of Nigeria
Cataloguing-in-Publication (CIP) Data

Z
678.9
.C883 Crystalizing Emerging Technologies, Trends and Perspectives in Librarianship: A Book of Readings in Honour of Professor Nse Emmanuel Akwang /by A. O. Unagha et al. Uyo: Inela Venture & Publishers Ltd, 2026.
xx, 365p, ills.; 26cm
Includes references and index
ISBN: 978-978-62560-8-5

1. Library Science - Technological Innovations
2. Libraries - Automation
3. Information Technology
4. Academic Libraries - Nigeria

i Title ii. C. A. Okezie iii. K. G. Oyeniran iv. C. O. Udofot

Z 678.9 .C883

ISBN: 978-978-62560-8-5

DORAND PUBLISHERS

PRINTED BY
Inela Venture & Publishers Ltd.
70 Dominic Utuk Avenue
Uyo
Akwa Ibom State
Nigeria.

EDITORIAL ADVISORY TEAM

Chapter Six

Blockchain Technologies as Innovative Tools for Managing Modern Libraries

Hussaini Musa (Ph.D)[1] & Ladan Dogara[2]
Corresponding Author: hussaini.musa@futminna.edu.ng +2348036201118
[1]University Library Services, Federal University of Technology, PMB 65 Minna, Niger State, Nigeria
[2]Department of Information Science, Makerere University | +234 807 666 7597

Abstract

The dynamic landscape of digital transformation has compelled libraries to adopt innovative technologies that enhance transparency, efficiency, and trust in information management. Blockchain technology, an immutable and decentralized ledger, presents immense potential for reengineering modern library operations beyond financial transactions. This chapter explores blockchain as an innovative tool for managing contemporary libraries, focusing on its applications in metadata authentication, digital rights management, interlibrary loan systems, and preservation of digital assets. By leveraging blockchain's core attributes decentralization, traceability, and immutability libraries can address persistent challenges such as data tampering, intellectual property infringements, and lack of interoperability among information systems. The discussion integrates insights from emerging research and global case studies to illuminate practical use cases and implementation pathways. It also examines barriers to adoption, including technological complexity, high initial costs, and limited policy frameworks, particularly within developing contexts. The chapter proposes a conceptual model for blockchain integration into library management systems, emphasizing collaborative partnerships, digital literacy development, and ethical data governance. In conclusion, blockchain technology emerges as a catalyst for transparent, secure, and future-oriented library services, aligning with the broader vision of innovation and sustainability in modern librarianship.

Keywords: Blockchain, Library Management, Information Security, Metadata Integrity, Emerging Technologies

Introduction

Libraries have undergone rapid transitions driven by technological innovation, information expansion, and shifts in user expectations. As society becomes increasingly digitized, libraries are expected to offer seamless access to information, support remote learning, and provide intelligent services that extend beyond traditional physical collections. These changes have intensified the need for emerging technologies capable of enhancing operational efficiency, strengthening information security, and supporting modern user behaviors (Singh, 2018). The growing complexity of digital information ecosystems characterized by large datasets, diverse formats, and distributed access models demands advanced infrastructures that can support interoperability and ensure the authenticity of digital resources.

Emerging technologies such as artificial intelligence (AI), machine learning, cloud computing, and the Internet of Things (IoT) are increasingly being integrated into library operations to streamline cataloguing, automate circulation tasks, and provide personalized

reference services (Bi et al., 2022). However, as digital information environments expand, libraries face heightened cybersecurity threats and concerns about the integrity, provenance, and long-term preservation of digital assets. This has created a pressing need for systems that provide transparency, decentralized control, and resistance to data manipulation.

Blockchain technology known for its distributed ledger architecture, immutability, and cryptographic security has attracted attention as a potential solution capable of addressing many of these challenges. Originally developed for financial applications, blockchain has since been explored in sectors requiring trusted information exchange, such as healthcare, government, and education (Yaga et al., 2019). Its relevance to libraries lies in its potential to secure digital records, authenticate information, and support decentralized resource sharing. The rationale for adopting blockchain within library management is therefore grounded in the need to build resilient, trustworthy, and future-ready information systems that align with the demands of a digitally networked society. In this context, an overview of digital transformation in librarianship provides a necessary foundation for understanding how emerging technologies are reshaping modern library management.

Overview of Digital Transformation in Librarianship

Digital transformation in libraries refers to the integration of digital technologies into all aspects of library services, fundamentally altering how information is delivered, accessed, and preserved. The shift began with automation tools and online catalogues, later evolving into digital repositories, electronic resource management systems, and sophisticated discovery platforms (Rahmanova, 2025). These developments were driven by rapid advancements in publishing technologies, the proliferation of e-resources, and the rise of remote access needs among academic and public library users.

Contemporary digital libraries employ cloud-based systems, AI-enhanced cataloguing tools, and data analytics to provide responsive, user-centered services. Personalized search recommendations, virtual reference assistants, and digital preservation infrastructures are now integral to modern library operations. Digital transformation has also encouraged libraries to operate as collaborative hubs by enabling shared metadata, joint acquisition programs, and collective digital preservation initiatives through consortium-based systems (Sandhu, 2018).

However, the shift to digital environments has introduced new challenges. Libraries must manage heterogeneous data formats, negotiate complex digital rights, and ensure the integrity and authenticity of digital content over long periods. Cybersecurity threats have grown more sophisticated, exposing vulnerabilities in traditional centralized systems. Furthermore, the rising dependence on commercial vendors for hosting, analytics, and authentication services increases issues related to data privacy, cost, and vendor lock-in (Kempf, 2023). As libraries navigate this ongoing digital transformation, new technological frameworks such as blockchain offer promising pathways to address these systemic challenges while enhancing transparency and collaboration. Against this backdrop of digital transformation in librarianship, the discussion now shifts to the tools that enable the effective management of modern libraries

Tools for Managing Modern Libraries

Modern library management relies on an ecosystem of digital tools designed to support cataloguing, circulation, acquisitions, authentication, and digital preservation. Integrated Library Systems (ILS) and Library Services Platforms (LSP), including Koha, Alma, Evergreen, and WorldShare Management Services, are widely used to automate core

functions such as metadata creation, serial management, and circulation tracking (Breeding, 2021). These systems provide centralized dashboards for library staff while enabling online access through user-facing interfaces.

Digital asset management systems and institutional repository platforms such as DSpace, EPrints, and Fedora are essential for managing scholarly outputs, digitized heritage materials, and electronic theses and dissertations. Libraries additionally employ discovery layers such as Primo, Summon, and VuFind to offer unified search experiences across multiple databases, increasing accessibility and improving user navigation.

Authentication and identity-management tools, including Shibboleth and OpenAthens, support secure, remote access to licensed digital resources. Meanwhile, cloud services, AI tools, and analytics dashboards provide new capabilities for resource optimization, automated classification, and understanding user behavior. While these tools have modernized library operations, they nonetheless rely largely on centralized architectures and vendor-controlled systems, leaving unresolved issues related to data integrity, interoperability, and long-term sustainability. Despite the growing adoption of digital tools in library management, persistent challenges remain unresolved, necessitating a clear statement of the problem addressed in this chapter.

Problem Statement

Despite major advances in digital infrastructure, current library management systems face limitations that hinder efficiency and innovation. Centralized databases used in most ILS and LSP platforms remain vulnerable to hacking, unauthorized alterations, and system-wide failures, exposing risks to user privacy and digital collection integrity (Singh et al., 2024). Interoperability challenges persist due to incompatible metadata standards, proprietary software structures, and restricted API access, making it difficult for libraries to share resources seamlessly across platforms. Additionally, libraries struggle with ensuring the authenticity and provenance of digital records, particularly in open-access repositories where content may be duplicated, altered, or misattributed. Issues in digital rights management, including opaque licensing agreements and inconsistent usage tracking, further complicate operations. These limitations highlight the need for emerging technologies such as blockchain to enhance transparency, security, and decentralized collaboration in library environments. Against this backdrop of persistent challenges in modern library management, the objectives and significance of exploring blockchain technology are outlined in the following section.

Primary Objective: The primary objective of exploring blockchain technology in library management is to examine how decentralized ledger systems can transform the security, reliability, and efficiency of library operations. This involves assessing the capacity of blockchain to create a secure, transparent, and tamper-resistant infrastructure that supports core library functions while addressing the limitations of traditional centralized management systems.

Specific Objectives: The specific objectives include identifying practical applications of blockchain within library environments, such as establishing tamper-proof cataloguing and metadata records, enabling authenticity verification of digital resources, managing digital rights through smart contracts, streamlining interlibrary loan transactions, and strengthening user identity management. Additionally, it seeks to evaluate how blockchain can enhance interoperability among library networks and improve data integrity, transparency, and operational trust.

Significance of the Study: The significance of exploring blockchain in library management lies in its potential to reduce vulnerabilities associated with centralized systems, enhance data security and authenticity, and foster transparent collaboration across institutions. By supporting secure digital preservation, improving accountability in transactions, and enabling innovative service delivery models, blockchain technology can position libraries as resilient, forward-looking institutions capable of meeting evolving information needs in an increasingly digital and interconnected society.

Theoretical Framework: Foundations for Blockchain Adoption in Library Management

1. Diffusion of Innovation Theory

The Diffusion of Innovation Theory was propounded by Everett M. Rogers in 2003.

Rogers (2003) defined diffusion as the process by which an innovation is communicated through certain channels over time among the members of a social system. He further posits that the rate and extent of adoption are largely influenced by five perceived attributes of an innovation: relative advantage, compatibility, complexity, trialability, and observability.

Relevance to the Study: The Diffusion of Innovation Theory provides a rigorous explanatory lens for examining the adoption of blockchain technology in library management. Within this framework, blockchain constitutes an innovation whose uptake depends on stakeholders' perceptions and institutional contexts. Its *relative advantage* is evident in its capacity to enhance data security, immutability, transparency, and decentralized trust mechanisms when compared with conventional centralized library systems. *Compatibility* relates to the extent to which blockchain aligns with existing bibliographic standards, metadata schemas, institutional policies, and professional values in librarianship. *Complexity* may impede adoption, particularly in environments characterized by limited technological infrastructure or inadequate technical expertise. Conversely, *trialability* is facilitated through pilot initiatives, consortium-based experiments, and phased implementation strategies, while *observability* is reflected in demonstrable improvements in record authenticity, digital rights management, and interlibrary transactions. Accordingly, DOI elucidates both the motivational and structural determinants influencing blockchain adoption decisions within library systems.

2. Socio-Technical Systems Theory

Socio-Technical Systems Theory was originally developed by Eric Trist and Fred Emery in 1951 at the Tavistock Institute, and further elaborated in later works.

Socio-Technical Systems Theory asserts that:

"Every organization comprises a social system and a technical system which must be jointly optimized for effective performance."

Relevance to the Study: Socio-Technical Systems Theory provides a complementary analytical framework by emphasizing the interdependence between technological infrastructures and social structures within organizations. In the context of blockchain implementation in libraries, the *technical subsystem* encompasses distributed ledger architecture, cataloguing platforms, authentication protocols, and digital preservation systems. The *social subsystem* includes librarians' competencies, professional norms, governance mechanisms, user expectations, and collaborative institutional relationships.

The theory underscores that the successful integration of blockchain is contingent upon the joint optimization of these subsystems. Technological deployment without corresponding adjustments in organizational culture, workflow design, staff training, and policy frameworks may generate resistance or suboptimal outcomes. Thus, STS theory situates blockchain adoption not merely as a technical upgrade but as an organizational transformation requiring systemic alignment and participatory change management.

Collectively, these theories establish a robust conceptual foundation for this study. Diffusion of Innovation Theory explains the dynamics influencing the acceptance and spread of blockchain technology among library stakeholders, while Socio-Technical Systems Theory elucidates the structural and organizational conditions necessary for its sustainable and effective integration.

Conceptual Framework

Description of the Proposed Blockchain-Enabled Library Management Model

The proposed conceptual framework advances a blockchain-enabled library management model that integrates distributed ledger technology with conventional library operations in order to strengthen data integrity, transparency, interoperability, and institutional trust. Within this model, libraries are reconceptualized not merely as custodians of information resources, but as interconnected nodes within a distributed knowledge ecosystem. In this ecosystem, critical records such as metadata, digital rights agreements, transaction logs, and user authentication credentials are cryptographically validated and recorded on a blockchain infrastructure, thereby ensuring immutability, provenance, and verifiability (Emmanuel et al., 2023).

At the architectural level, the framework adopts a permissioned blockchain model, which is particularly appropriate for library consortia and institutional networks where governance, access control, and privacy protection are paramount. Unlike public blockchains that allow unrestricted participation, permissioned ledgers limit validation and participation rights to authorized institutions. This design ensures that sensitive data such as patron records, lending histories, and rights metadata remains protected while still benefiting from decentralized consensus, auditability, and cryptographic security (Swan, 2015). Such an approach aligns with prevailing data protection regulations, including the General Data Protection Regulation (GDPR), and comparable regional privacy frameworks.

The framework is organized around five interrelated functional domains:

1. Metadata and Cataloguing

Bibliographic records, authority data, and special collections metadata are hashed and anchored to the blockchain ledger. Each modification generates a timestamped transaction, thereby creating a permanent and verifiable audit trail. This mechanism enhances provenance tracking, prevents unauthorized alterations, and strengthens trust in shared cataloguing environments.

. Digital Rights Management

icensing agreements, access permissions, and usage conditions are embedded within smart ntracts that automatically execute predefined rules. By automating compliance and forcement, the system reduces administrative overhead and minimizes disputes related to ess and copyright management (Viji et al., 2025).

3. Resource Sharing and Interlibrary Loans

Interlibrary loan requests, approvals, transfers, and returns are recorded as blockchain transactions. This produces a transparent and tamper-resistant record of resource exchanges across participating institutions, improving accountability, reducing disputes, and enhancing collaborative efficiency.

4. User Identity Management

The framework incorporates decentralized identity mechanisms, whereby patrons are assigned decentralized identifiers (DIDs). Authentication credentials are cryptographically verified without central storage of sensitive personal data. This enhances privacy, enables secure cross-institutional access, and reduces vulnerabilities associated with centralized identity repositories (Kareklas & Chaleplioglou, 2025).

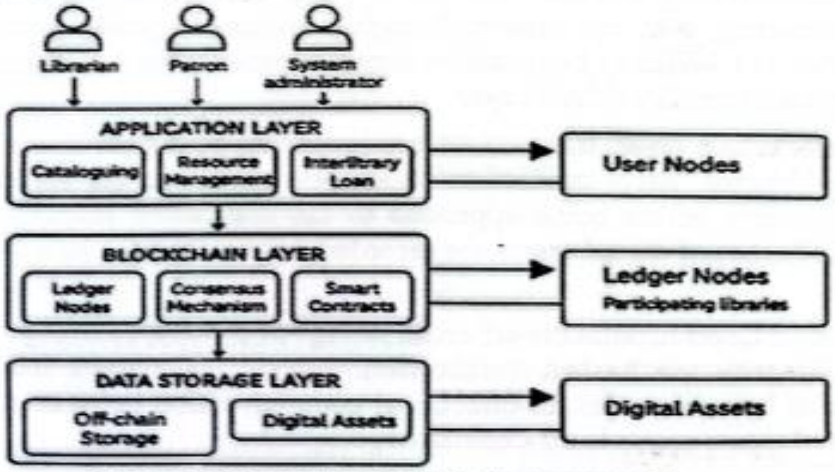
5. Digital Preservation

To address scalability and storage limitations, the framework adopts a hybrid on-chain/off-chain model. Cryptographic hashes of digital objects are stored on-chain to guarantee authenticity and integrity, while the full digital content resides in distributed or institutional repositories. This approach ensures tamper-evident preservation without overburdening the blockchain network.

Structural Characteristics of the Framework

The proposed model emphasizes modularity and interoperability, allowing seamless integration with existing Integrated Library Systems (ILS), digital repositories, and discovery platforms. By positioning blockchain as a verification and governance layer rather than a replacement for existing infrastructure, the framework minimizes operational disruption while enhancing trust, security, and collaborative governance (Di Vaio et al., 2025).

In summary, the conceptual model (Figure 1) situates blockchain as an enabling infrastructural layer that augments core library functions cataloguing, digital rights enforcement, resource sharing, identity management, and digital preservation through decentralized validation, immutability, and distributed trust mechanisms. This layered approach ensures both technological robustness and organizational adaptability within contemporary digital library ecosystems.



Conceptual framework for Blockchain-Library management

Components and Interaction Between Blockchain Layers and Library Subsystems

The framework in figure 1 is structured in three interrelated layers, each interacting with traditional library subsystems:

1. Application Layer: Interfaces used by librarians, patrons, and system administrators, including cataloguing tools, resource management dashboards, DRM interfaces, and API clients. User actions in this layer (e.g., borrowing a book, updating metadata, or accessing a digital resource) trigger blockchain transactions.
2. Blockchain Layer: The core decentralized ledger, maintaining transaction history, metadata hashes, smart contracts, and decentralized identity records. Key components include:
    a. Ledger Nodes: Each participating library operates a node, maintaining a copy of the ledger and validating transactions.
    b. Consensus Mechanism: A permissioned consensus algorithm (e.g., Practical Byzantine Fault Tolerance, PBFT) ensures data integrity and agreement across nodes.
    c. Smart Contracts: Automate business logic, including DRM enforcement, loan processing, and preservation validation.
3. Data Storage Layer: Off-chain repositories store actual content (e-books, multimedia, digitized manuscripts) to address scalability and performance constraints. Hashes of these assets are anchored on-chain to ensure authenticity and integrity.

Interactions: When a librarian adds a new bibliographic record, the application layer sends the data to the blockchain layer, where it is hashed and recorded. Smart contracts verify compliance with cataloguing standards and trigger notifications to other nodes. Similarly, when a patron requests a digital resource, the identity is validated via decentralized credentials, and the transaction is logged immutably. Resource access and rights enforcement are monitored automatically, while the actual file remains in off-chain storage.

The model ensures synchronized metadata, transparent transactions, secure user identity, and auditable digital preservation, while enabling interoperability with legacy library systems and external consortia networks.

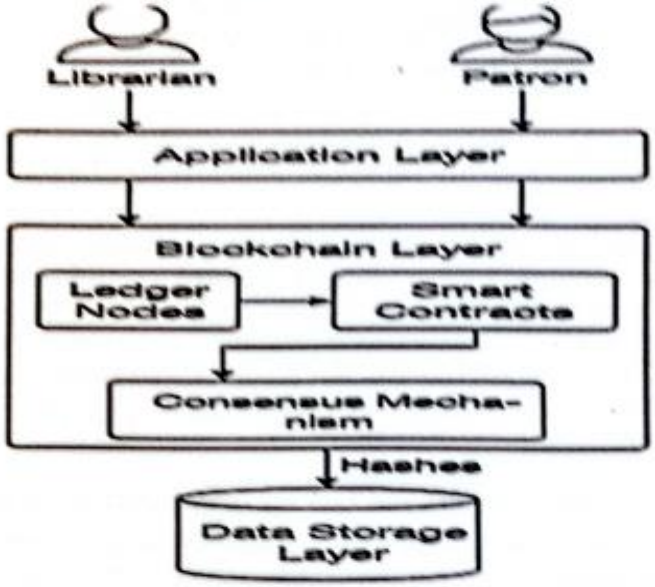
The conceptual diagram in figure 1 & 2 represents data flow and interactions within the blockchain-enabled library system. At the top, the User Nodes represent patrons and librarians interacting with the system through applications (cataloguing interfaces, e-resource portals, ILL systems). User actions trigger requests to the Application Layer, which communicates with the Blockchain Layer.

Within the blockchain layer, transactions are processed by ledger nodes maintained by participating libraries. Each transaction undergoes validation via smart contracts and consensus protocols before being appended to the distributed ledger. Simultaneously, cryptographic hashes of digital assets are recorded, anchoring off-chain files in a tamper-proof manner.

The Data Storage Layer handles the off-chain storage of content, ensuring scalability while preserving integrity via hashed verification. Interaction arrows indicate real-time synchronization between nodes, bi-directional communication between applications and blockchain, and secure access to off-chain storage.

The diagram in figure 2 illustrates the holistic flow: user interactions trigger blockchain-validated actions, smart contracts enforce rules, nodes maintain consensus, and off-chain storage preserves content. This visual emphasizes decentralization, immutability, auditability, and interoperability, while demonstrating practical integration with library operations.

Figure 2: Blockchain Library Management Framework



Concept of Blockchain Technology: Origin, Components, and Mechanisms

Blockchain technology emerged from the quest to develop a decentralized digital currency. Its conceptual origin is attributed to Nakamoto's (2008) seminal white paper introducing Bitcoin, a peer-to-peer electronic cash system that eliminated the need for trusted intermediaries. While blockchain gained prominence through cryptocurrency, scholars and industries soon recognized its potential as a secure, transparent, and tamper-resistant system for managing digital records beyond financial transactions (Crosby et al., 2016).

A blockchain is essentially a distributed ledger a synchronized database maintained across multiple network nodes. Its architecture consists of several key components. First, data are stored in blocks, each containing a timestamp, transaction records, and a cryptographic hash linking it to the previous block. This chain-link structure ensures that altering a single block would require modifying all subsequent blocks across all copies of the ledger, rendering unauthorized tampering extremely difficult (Yaga et al., 2019).

Second, the system operates through nodes, independent computers participating in the network. Each node maintains a full or partial copy of the ledger and verifies new transactions based on predefined protocols. This decentralized arrangement eliminates reliance on a central authority, thereby improving resilience and transparency (Hughes et al., 2019).

The third essential element is the consensus mechanism the procedure by which nodes agree on the validity of transactions. Common mechanisms include Proof of Work (PoW), which

requires nodes to solve computationally intensive puzzles; Proof of Stake (PoS), which selects validators based on stake ownership; and Practical Byzantine Fault Tolerance (PBFT), designed for permissioned networks that require stronger consistency and efficiency (Zheng et al., 2017). These consensus algorithms form the backbone of blockchain's integrity, ensuring that all participating nodes share an identical and trustworthy record.

Blockchain systems are categorized into public, private, and consortium blockchains. Public blockchains such as Bitcoin and Ethereum allow unrestricted participation, whereas private blockchains limit access to authorized nodes, making them suitable for organizational environments. Consortium blockchains combine both features and allow multiple institutions to jointly govern the ledger (Xu et al., 2017).

Beyond cryptocurrencies, blockchain supports smart contracts, self-executing agreements encoded with conditional logic. Smart contracts automate processes such as authentication, licensing, or transaction logging, reducing administrative overhead and minimizing human error (Swan, 2015).

Overall, blockchain offers a platform for secure, decentralized information management. Its key properties immutability, transparency, distributed control, and cryptographic verification make it increasingly relevant for sectors requiring trustworthy recordkeeping, including healthcare, supply chain management, education, and library science. Building on the conceptual and theoretical background, this section examines established theories of innovation and technology adoption that provide insight into the acceptance and implementation of blockchain in modern libraries.

Link Between Blockchain Principles and Library Information Management

Blockchain's foundational attributes correspond directly to core functions of library information management. Immutability ensures that cataloguing metadata and bibliographic records cannot be illicitly altered, supporting record integrity and traceability key requirements for academic and cultural heritage institutions (Xu & Zhang, 2023). Decentralization facilitates collaborative cataloguing, resource sharing, and distributed digital preservation across library consortia, reducing reliance on proprietary centralized systems.

Transparency and provenance tracking strengthen the authenticity of digital assets, enabling libraries to document the history, ownership, and versioning of electronic resources. This is particularly important for digital scholarship, special collections, and archival materials. Blockchain's smart contracts can streamline interlibrary loan processes, automate digital rights management, and enforce licensing terms with greater precision and accountability.

Furthermore, blockchain enhances user identity management by enabling secure authentication processes that protect patrons' privacy more effectively than centralized databases. By distributing control, blockchain reduces vulnerabilities associated with single-point failures and unauthorized access.

Overall, blockchain's alignment with library values trust, preservation, access, and stewardship positions it as a compelling tool for modernizing library information systems. Its principles address persistent challenges in authenticity verification, data security, interoperability, and long-term preservation, making it a promising innovation for library management in the digital age. Building on these theoretical foundations that explain innovation and technology adoption, the next section shifts from conceptual perspectives to

collections, inter-library loan voucher systems, and secure library card or credential verification.

Empirical studies also support these claims. A recent work focusing on Nigerian libraries underscored how blockchain could address prevalent security and data integrity challenges in digital collection management particularly problems arising from centralized cataloguing systems, unauthorized access, weak logging mechanisms, and insufficient encryption (Emmanuel et al., 2023). Another study conducted in a different context demonstrated how blockchain technology can improve information retrieval and search efficiency in library systems. This study highlighted the ability to create traceable and immutable metadata and indexing records, which enhances retrieval reliability and user trust in digital library environments.

In the archival domain, blockchain has also been utilized to secure and verify the authenticity of digital archival assets. For example, a project known as ARCHANGEL implemented a blockchain-based system to preserve video archives. The system used temporal content hashes (TCHs) to represent content in a way that remained invariant under encoding changes, enabling long-term verification of integrity regardless of format transformations a critical requirement for archives undergoing format migration over time. Similarly, the archival system ARCHAIN was proposed for state-level archives in Russia, using blockchain to record document-transfer events and preserve archival history in an immutable ledger (Galiev et al., 2018).

These use cases illustrate that blockchain has practical relevance to the fundamental functions of libraries and archives: cataloguing, preservation, access control, resource sharing, and provenance validation. As the volume and complexity of digital resources grow, blockchain-based systems may provide robust infrastructures for trustworthy, collaborative, and long-term information management. Following the examination of blockchain use cases in libraries, archives, and digital repositories, the discussion progresses to a comparative analysis of blockchain and traditional digital record systems, highlighting their differences in functionality, security, scalability, and implications for information management.

Comparative Analysis: Blockchain vs. Traditional Digital Record Systems

Traditional digital record systems, such as relational databases or centralized repository platforms, have been the backbone of libraries and archives for decades. These systems enable efficient cataloguing, indexing, content storage, and access control. However, a growing body of work recognizes their limitations: centralization creates a single point of failure, making systems vulnerable to hacking, unauthorized alteration, data loss, or corruption (Ahmad, 2024). Moreover, traditional systems may struggle with interoperability across different institutions, as metadata standards, software platforms, and licensing agreements often vary widely.

Blockchain-based systems offer a fundamentally different approach. First, their distributed ledger architecture ensures that data are replicated across many nodes, eliminating single-point-of-failure risks and increasing resilience (TechTarget, 2025). Second, immutability and cryptographic hashing guarantee that once a record is added, it cannot be altered without detection a property that significantly improves data integrity and provenance tracking compared to traditional databases that allow edits and deletions. Third, blockchain facilitates transparent audit trails, so any change or access to records is visible to all authorized participants, enhancing accountability and trust (Hughes et al., 2019).

Additionally, blockchain enables smart contracts self-executing code that can automate processes such as licensing, interlibrary loans, access permissions, and usage tracking. Such automation reduces administrative overhead and the potential for human error, contrasting with manual or semi-automated workflows in legacy systems (Ahmad, 2024).

However, it is not that blockchain uniformly outperforms traditional systems. Blockchain does not inherently store large digital objects efficiently a significant limitation for libraries and archives dealing with multimedia or large batches of digitized materials. As noted in studies of digital preservation, a hybrid approach is often required: metadata stored on-chain, while bulky content is stored off-chain (e.g., in conventional storage), with hashes linking back to the blockchain for verification (Werthmuller, 2025). Also, traditional systems currently benefit from mature ecosystems (standards, protocols, tool support), whereas blockchain-based library systems are relatively nascent and may face scalability, interoperability, and sustainability challenges.

In sum, while blockchain offers compelling advantages decentralization, integrity, transparency, and automation traditional systems remain more efficient for raw storage and bulk data handling, and benefit from long-established standards and broad community support. The strengths and limitations of each suggest that blockchain may serve best as a complementary technology rather than a wholesale replacement. Drawing on the comparative analysis of blockchain and traditional digital record systems, the discussion now turns to gaps and opportunities identified in previous studies, highlighting unresolved challenges, underexplored contexts, and emerging directions for future research and practice.

Gaps and Opportunities Identified from Previous Studies

Despite growing interest, the literature reveals several gaps and areas needing further research and development before blockchain can be widely adopted in library and archival settings. A bibliometric analysis of blockchain implementation in digital archives between 2015 and 2023 found a relatively small number of publications (106 documents) and noted that research linking blockchain with archives remains "not very developed." This suggests that empirical evidence and practical pilot projects remain limited, especially for non-Western contexts or developing countries.

Furthermore, studies frequently highlight challenges such as scalability (storing large or multimedia files), cost and energy consumption, and governance complexity, especially in consortium-based or cross-institutional blockchain networks (Werthmuller, 2025). In contexts like Nigeria, additional obstacles arise: infrastructural constraints, limited technical capacity among library staff, and financial limitations all of which may hinder adoption (Tella, Amuda & Ajani, 2022).

Moreover, there is a lack of standardized models, best practices, or frameworks tailored to library and archival institutions. Few studies provide detailed architectural blueprints or sufficiently address legal and ethical concerns such as data privacy, especially relating to user identity and compliance with data protection laws (Kareklas & Chaleplioglou, 2025).

These gaps present opportunities for future research: empirical evaluation of blockchain-based library systems, pilot implementations in diverse institutional contexts (especially developing countries), development of hybrid on-chain/off-chain models optimized for large digital collections, and establishment of governance, policy, and standardization frameworks to guide ethical and sustainable adoption. Building on the gaps

opportunities identified in previous studies, the discussion now shifts to blockchain applications in library management, focusing on how blockchain can be strategically integrated into core library operations, services, and administrative processes.

Blockchain Applications in Library Management

Metadata and Cataloguing Integrity

One of the cores promises of blockchain in library management lies in strengthening the integrity, authenticity, and traceability of metadata and cataloguing records. Traditional cataloguing and metadata systems even when digital often rely on centralized databases controlled by a single institution or vendor. This centralization can expose bibliographic data to unauthorized modifications, accidental corruption, or loss, especially in multi-institution collaboration or long-term preservation contexts (Emmanuel, et al., 2023).

By contrast, a blockchain-based cataloguing system stores metadata records in a distributed ledger that is replicated across participating nodes. Each cataloguing entry whether a new book, a digitized manuscript, or a special collection item can be hashed and recorded, with a timestamp and provenance data (e.g., who catalogued it, when, version history). Once entered, such metadata becomes immutable, meaning alterations or deletions are impossible without detection. This ensures a permanent audit trail of changes, supporting trust in cataloguing quality and historical fidelity (Emmanuel, 2023).

Moreover, in collaborative library networks or consortia where multiple libraries contribute to a shared catalogue or union catalogue blockchain facilitates distributed, synchronized metadata management without relying on a single central server. This reduces risk of data inconsistency, data divergence, or "single point of failure." A study integrating blockchain with CryptoJS in digital libraries highlighted enhanced security and transparency in cataloguing and book-transaction records (Evwiekpaefe et al., 2025).

Thus, blockchain supports catalogue integrity, provenance tracking, and collaborative cataloguing valuable capabilities for modern libraries managing growing, distributed, and hybrid (physical + digital) collections.

Digital Rights and Intellectual Property Management

Digital Rights Management (DRM) and intellectual property (IP) protection are crucial for libraries especially those offering e-books, digitized manuscripts, multimedia resources, institutional research outputs, or licensed electronic content. Traditional DRM systems often rely on centralized license servers, proprietary access control, and may lack transparency, making auditing and verifying rights usage difficult (Tamilselvan, 2024).

Blockchain offers a compelling alternative by enabling smart-contract–based DRM frameworks, in which licensing terms, access conditions, expiration dates, and usage permissions are encoded in self-executing contracts on the ledger (Viji, et al., 2025). Under such a system, once a user is granted access (or a library acquires a digital asset), the transaction is recorded immutably. Any subsequent access, duplication, or distribution attempt is traceable, providing provenance for digital materials and ensuring that usage adheres to agreed terms.

Some proposals combine blockchain with perceptual hashing, watermarking, or distributed file storage to enhance IP protection. For instance, the "SecureRights" framework stores

watermark or hash information along with timestamp authentication to defend against unauthorized use or tampering (Madushanka, et al., 2024).

For libraries, such systems enable transparent, accountable, and secure digital content distribution, benefiting both authors/publishers and users by safeguarding rights while facilitating controlled access. DRM becomes less opaque and more trustworthy, reducing risk of license violation, piracy, or unauthorized redistribution.

Interlibrary Loan and Resource Sharing

Interlibrary Loan (ILL) and resource sharing have long been central functions of modern libraries, allowing institutions to broaden access to resources beyond their local holdings. However, traditional ILL systems often involve substantial administrative overhead, manual transaction records, delayed tracking, and trust-based transfers especially when multiple institutions are involved (Tella et al., 2022).

Blockchain can streamline ILL and resource sharing by enabling decentralized, transparent, and auditable transactions across participating libraries. ILL requests, lending records, return confirmations, and digital resource sharing can be recorded on the ledger. Each transaction becomes a block with verifiable metadata: who borrowed, when, from which library, due dates, and status updates. Because the ledger is distributed, all participating institutions share a synchronized transaction history, reducing duplication, miscommunication, or loss of records.

Some conceptual studies envision a "distributed library ecosystem" where patrons or libraries can transfer resources (physical or digital) without centralized gateways, using blockchain as the trust layer (Hasan & Sanjay, 2020). Such a decentralized ILL model fosters efficiency, reduces delays, and improves accountability. Moreover, blockchain enables tamper-resistant management of shared ownership, access rights, circulation records, and inter-institutional collaboration, offering a "library consortium 2.0" infrastructure that is transparent and sustainable.

User Identity and Access Management

User identity, authentication, and access control are fundamental to library services especially in digital contexts, when patrons remotely access e-resources, institutional repositories, or licensed databases. Traditional identity management systems (centralized servers, SSO frameworks) may expose libraries to risks such as unauthorized access, data breaches, and privacy violations. Synchronization across consortium networks can also be error-prone.

Blockchain provides decentralized identity (DID) models and secure, immutable access logs. According to the San Jose State University School of Information, blockchain could enable "sovereign identity," giving users control over their digital identities, enhancing privacy, and preventing identity theft (Meth, et al., 2019).

In a blockchain-based system, credentials need not be stored centrally; identity proofs (cryptographic tokens) are logged on the ledger. Access to digital resources borrowings, downloads, renewals is immutable, creating an audit trail across the network. Blockchain-based identity also allows portable, interoperable user identities, enabling seamless cross-institution access without redundant registration.

Preservation of Digital Assets

Digital preservation maintaining long-term accessibility of digital assets including e-books, manuscripts, multimedia, research outputs, and archival materials remains a persistent challenge. Traditional preservation relies on centralized repositories, backups, format migration, and trust in institutional infrastructure, all vulnerable to failure, tampering, or obsolescence.

Blockchain provides a tamper-proof, decentralized preservation infrastructure. Projects like ARCHANGEL use temporal content hashing (TCH) to store content fingerprints on a permissioned blockchain, ensuring any future alterations are detectable (Bui et al., 2019). ARCHAIN similarly records archival events and custody changes, providing a verifiable audit trail (Bui et al., 2019).

Libraries can store metadata and hashes on-chain while storing large assets off-chain. Verification is simple: recompute the hash and compare with the blockchain record. This reduces risk of undetected corruption, tampering, or data loss, and supports cooperative archiving among institutions, enhancing resilience and aligning with the collaborative ethos of libraries.

Blockchain applications in metadata integrity, DRM, interlibrary loan, user identity, and digital preservation offer opportunities to address weaknesses of traditional systems. By leveraging decentralization, immutability, transparency, and cryptographic security, libraries can build resilient, trustworthy, and collaborative infrastructures for the digital era. Pilot projects and conceptual frameworks (e.g., ARCHANGEL) demonstrate potential for next-generation librarianship, enabling secure resource sharing, rights management, and long-term preservation.

Implementation Challenges and Considerations

Technical Barriers

Despite the considerable promise of blockchain for libraries, the technical challenges to implementing blockchain-based library management systems are substantial. First, scalability remains a major concern. Many blockchain networks especially public blockchains using resource-intensive consensus mechanisms like Proof-of-Work (PoW) struggle to handle high transaction volumes or large data loads efficiently. In contexts such as library cataloguing, resource sharing or digital preservation where many transactions or large metadata records might be involved, this limitation could cause unacceptable delays or system bottlenecks (Di Vaio et al., 2025; Messina, et al., 2025).

Second, integration with existing legacy systems presents difficulties. Most libraries already use established Integrated Library Systems (ILS), digital repositories, authentication mechanisms, and database systems. Retrofitting a blockchain layer often requires extensive customization, development of interfaces and migration of existing data a process that is both technically complex and risky (ALA TechSource, 2023).

Third, blockchain's computational and infrastructural demands can be prohibitive. Consensus mechanisms, cryptographic operations, and distributed ledger maintenance require reliable servers, stable power supply, and robust network connectivity resource requirements that may exceed what many libraries, especially in resource-constrained settings, can sustain (Messina, et al., 2025).

Finally, there are security and reliability concern intrinsic to blockchain implementations: vulnerabilities in smart contracts, potential software bugs, and dependency on all participating nodes to maintain system integrity. In some cases, network attacks or bugs can undermine trust in the system a critical issue for institutions entrusted with preserving scholarly and cultural heritage (Di Vaio et al., 2025).

Because of these technical barriers, transitioning from conventional library management systems to blockchain-based ones are nontrivial and requires careful planning, robust infrastructure, and expert capacity.

Economic and Policy Challenges (especially in Developing Countries)

In developing countries, libraries often operate under constrained budgets and limited infrastructural support. The cost of implementation and maintenance of a blockchain-based system can be prohibitively high. According to a study on the relevance of blockchain in libraries and archives in Nigeria, many institutions lack the financial resources, stable power supply, and ICT infrastructure required to support distributed ledger systems making adoption unrealistic without external funding or governmental support (Tella, Amuda & Ajani, 2022).

Moreover, regulatory and policy uncertainty poses a significant obstacle. The regulatory environment surrounding blockchain is still evolving globally, and in many developing countries there is no clear legal framework for data storage, digital identity, or digital assets on distributed ledgers. This ambiguity discourages institutional commitment and long-term investment (HeLaLabs analysis, 2024).

Another economic challenge is return on investment (ROI) and sustainability. Libraries must weigh the benefits of blockchain (e.g. security, interoperability, preservation) against ongoing costs including hardware, energy consumption, maintenance, and potentially higher staffing costs due to need for specialized skills (ALA TechSource, 2023).

Finally, in developing context, infrastructure deficits (unreliable electricity, limited broadband, insufficient server capacity) further elevate costs and risk. Without stable infrastructure, the distributed and synchronized nature of blockchain becomes difficult to guarantee, undermining its effectiveness (Messina, et al., 2025; Tella et al., 2022).

Thus, for many libraries in economically constrained settings, economic viability and supportive policy framework are critical preconditions without which blockchain implementation may remain aspirational.

Ethical and Privacy Concerns

While blockchain's transparency and immutability are strengths for record-keeping and provenance, they also raise ethical and privacy challenges especially when personal or sensitive data (e.g., user identities, borrowing history, access logs) are involved. The immutable nature of blockchain conflicts with data protection regulations such as the right to erasure or data modification (e.g., under data protection laws) (Kareklas & Chaleplioglou, 2025).

Public or permissionless blockchains pose additional risks, since data added to the ledger becomes accessible to all participating nodes, potentially exposing user data to unauthorized parties. Libraries handling patron information must ensure confidentiality and compliance with data-privacy standards a requirement that complicates public ledger use (Kareklas &

Chaleplioglou, 2025).

Moreover, permanence of data may conflict with ethical obligations. For instance, libraries may need to remove or update personal data (e.g., upon user request), or anonymize records after certain period but immutability resists such modifications. Some scholars argue that this tension undermines user privacy and institutional responsibility (Politou, Casino, Alepis, & Patsakis, 2019).

Therefore, any blockchain-based library system must carefully consider what types of data are stored on-chain possibly restricting personal data to off-chain storage, using anonymization or pseudonymization, or employing privacy-preserving cryptographic techniques to reconcile blockchain's permanence with ethical and legal obligations.

Capacity Building and Training for Librarians

Implementing blockchain in libraries requires specialized technical expertise, including knowledge of distributed ledger technology, smart-contract development, cryptographic hashing, network maintenance, and data security. However, according to surveys and empirical studies, most library staff currently lack familiarity with blockchain or view it solely through the lens of cryptocurrency, limiting institutional readiness to adopt the technology (Tella, Amuda & Ajani, 2022; Advance Journal report, 2025).

In addition, maintaining blockchain systems involves ongoing tasks server maintenance, ledger synchronization, security auditing, and possibly smart contract updates which require sustained commitment. For many libraries, especially those in developing contexts, attracting and retaining skilled personnel is difficult due to limited budgets and non-competitive salaries (ALA TechSource, 2023).

To address this gap, capacity-building initiatives are essential. Libraries may need to collaborate with universities, technical institutes, or development agencies to provide training in blockchain architecture, system administration, and data governance. Pilot projects could serve as training grounds and expose librarians to practical implementation challenges creating institutional learning and building a community of practice (Messina, et al., 2025; HeLaLabs, 2024).

Future Prospects and Policy Implications

Blockchain in the Future of Smart Libraries

The integration of blockchain technology into library management has the potential to significantly transform libraries into smart, decentralized, and highly collaborative knowledge hubs. Smart libraries are characterized by real-time data-driven operations, enhanced interoperability among institutions, and seamless digital services for patrons (Di Vaio et al., 2025). Blockchain complements this vision by providing immutable records, decentralized verification, and automated enforcement of policies through smart contracts.

In the near future, blockchain-enabled smart libraries could offer autonomous cataloguing systems, where metadata updates, authority control, and bibliographic verification occur automatically across distributed networks. Patrons could seamlessly access digital and physical resources across multiple libraries using decentralized digital identities, eliminating redundant registration while ensuring privacy and security (Kareklas &

Chaleplioglou, 2025).

Moreover, blockchain can enhance digital preservation through decentralized, tamper-proof repositories where digital collections are jointly maintained by multiple institutions. This reduces dependency on a single custodian and mitigates risks associated with institutional failure, cyberattacks, or data corruption (Bui, 2019). Interlibrary loans, digital rights management, and access control could be automated using smart contracts, increasing efficiency, reducing administrative overhead, and improving accountability.

The evolution of smart libraries supported by blockchain also opens opportunities for innovative services, including micro-lending of digital resources, traceable content sharing, and reward mechanisms for knowledge contributions. Blockchain-based analytics could provide libraries with secure, aggregated insights into usage patterns while maintaining individual privacy. In essence, blockchain could underpin the next generation of knowledge ecosystems, where transparency, trust, and collaboration are built into the fabric of library operations.

Implications for Policy, Standards, and Library Education

The adoption of blockchain in library systems necessitates policy reform, standardization, and capacity building. Policies must address privacy, data protection, intellectual property, and ethical use of blockchain-managed records. For instance, national and regional regulations such as GDPR, HIPAA, or local data sovereignty laws must guide how patron identities, access logs, and digital collections are stored and shared on distributed ledgers (Swan, 2015).

Standardization is critical to ensure interoperability between different blockchain platforms, library management systems, and digital repositories. This includes developing metadata schemas, smart contract protocols, and consensus mechanisms suitable for library operations. International organizations like IFLA and ISO could play a role in creating guidelines for blockchain-based library infrastructures, facilitating cross-institutional collaboration and global adoption.

For library education, curricula must evolve to include blockchain literacy, decentralized data management, and smart contract programming alongside traditional library science competencies. Librarians will need to develop expertise in blockchain architecture, digital preservation, cryptography, and privacy-compliant identity management (Emmanuel et al., 2023). Training programs and professional development initiatives should emphasize both technical proficiency and ethical awareness, equipping librarians to act as intermediaries between emerging technologies and users while maintaining the principles of information access and stewardship.

Recommendations for Pilots, Partnerships, and Open Innovation

To advance blockchain adoption in libraries, pilot projects should be initiated within consortia or regional networks, testing real-world use cases such as metadata integrity, digital rights management, and interlibrary lending. Pilots should incorporate feedback mechanisms and measurable success indicators to refine blockchain models before large-scale implementation (Emmanuel, etal., 2023).

Partnerships with technology providers, academic institutions, and blockchain research centers can provide libraries with technical expertise, shared infrastructure, and access to innovative solutions. Collaborative research can foster open innovation, enabling libraries to

co-develop frameworks, smart contracts, and digital preservation protocols.

By adopting a phased, collaborative approach, libraries can mitigate risks, optimize resources, and accelerate innovation, ensuring that blockchain integration supports sustainability, transparency, and equitable access in the evolving landscape of digital librarianship.

Conclusion

This paper has explored the potential of blockchain technology as an innovative tool for managing modern libraries. Beginning with the challenges faced by traditional library management systems including centralized metadata control, limited interoperability, data security risks, and challenges in digital rights enforcement it highlighted the need for decentralized, tamper-proof, and transparent solutions (Emmanuel, etal., 2023). The study examined the conceptual and theoretical foundations of blockchain, emphasizing its components (blocks, nodes, consensus mechanisms) and relevant frameworks such as Diffusion of Innovation Theory and Socio-Technical Systems Theory, which underpin technology adoption in library settings (Swan, 2015; Kareklas & Chaleplioglou, 2025).

Through a detailed review of literature and case studies, the paper demonstrated how blockchain can strengthen metadata and cataloguing integrity, secure digital rights and intellectual property, improve interlibrary loan and resource sharing, enhance user identity and access management, and ensure the preservation of digital assets. The proposed conceptual framework integrates blockchain with existing library subsystems, employing permissioned ledgers, smart contracts, decentralized identity management, and off-chain storage to create an interoperable, secure, and resilient library ecosystem (Di Vaio, Palladino, & Varriale, 2025).

Additionally, the paper addressed the technical, economic, ethical, and educational considerations required for successful implementation, highlighting the need for policy guidance, standards, professional training, and pilot initiatives. This comprehensive analysis provides a roadmap for leveraging blockchain to enhance library operations and digital resource management.

Blockchain stands out as a transformative technology capable of driving innovation, fostering transparency, and ensuring sustainability in librarianship. By providing immutable records, decentralized governance, and automated enforcement of policies through smart contracts, blockchain enhances trust among institutions, patrons, and content providers. It enables collaborative, resilient, and secure management of library assets while supporting long-term digital preservation and interoperable access. As libraries increasingly operate across networks and digital ecosystems, blockchain offers a foundation for next-generation, smart libraries, where knowledge sharing, resource accessibility, and responsible stewardship are embedded into technological infrastructure (Swan, 2015; Bui, 2019).

References

Ahmad, M. I. (2024). Use of blockchain technology in library. *Synergy: International Journal of Multidisciplinary Studies*, 1(2), 9–14.

Ahmad, M. I. (2024). Use of Blockchain Technology in Library. *Synergy: International Journal of Multidisciplinary Studies*, *1*(2), 9-14. Retrieved from https://sijmds.com/index.php/pub/article/view/15

Bi, S., Wang, C., Zhang, J., Huang, W., Wu, B., Gong, Y., & Ni, W. (2022). A survey on artificial intelligence aided internet-of-things technologies in emerging smart libraries. *Sensors*, *22*(8), 2991. https://doi.org/10.3390/s22082991

Breeding, M. (2021). 2021 Library Systems Report. *American Libraries*, *52*(5), 22-33.

Bui, T., Cooper, D., Collomosse, J., Bell, M., Green, A., Sheridan, J., & Thereaux, O. (2019). ARCHANGEL: Tamper-proofing video archives using temporal content hashes on the blockchain. *arXiv*. https://arxiv.org/abs/1904.12059

Bui, T., Cooper, D., Collomosse, J., Bell, M., Green, A., Sheridan, J., ... & Brown, A. (2019). Archangel: Tamper-proofing video archives using temporal content hashes on the blockchain. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops* (pp. 0-0).

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, *36*, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Emmanuel, V. O., Efemini, M., Yahaya, D. O., & Oladokun, B. D. (2023). Application of blockchain technology to 21st century library services: Benefits and best practices. *Data and Metadata*, *2*, 59-59. https://doi.org/10.56294/dm20235

Emmanuel, V. O., Efemini, M., Yahaya, D. O., & Oladokun, B. D. (2023). Application of blockchain technology to 21st century library services: Benefits and best practices. *Data and Metadata*, *2*, 59-59.

Evwiekpaefe, A. E., Chinyio, D. T., Ajakaiye, F., & Aleke, P. O. (2025). A Blockchain-Based Digital Library System Integrated with CryptoJS for Enhanced Security and Transparency. *Journal of Information Systems and Informatics*, *7*(3), 2229-2244. DOI: 10.51519/journalisi.v7i3.1176

Galiev, A., Prokopyev, N., Ishmukhametov, S., Stolov, E., Latypov, R., & Vlasov, I. (2018, October). Archain: A novel blockchain based archival system. In *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)* (pp. 84-89). IEEE. DOI: 10.1109/WorldS4.2018.8611607

Hasan, N. (2020). Blockchain technology and its application in libraries. *Library Herald*, *58*(4), 118-125. DOI: 10.5958/0976-2469.2020.00030.10

Himeur, Y., Sayed, A., Alsalemi, A., Bensaali, F., Amira, A., Varlamis, I., ... & Dimitrakopoulos, G. (2022). Blockchain-based recommender systems: Applications, challenges and future opportunities. *Computer Science Review*, *43*, 100439. https://doi.org/10.1016/j.cosrev.2021.100439

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International journal of information management*, *49*, 114-129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

Kareklas, N., & Chaleplioglou, A. (2025). Innovations and Contradictions in Applying Blockchain Technology in Records Management under General Data Protection Regulation. *Journal of Integrated Information Management, 10*(1), 49-58. https://doi.org/10.26265/jiim.v10i1.41216

Kempf, K. (2023). Moving libraries toward digital transformation. *International Information & Library Review*, 55(3), 233-240. https://www.tandfonline.com/doi/abs/10.1080/10572317.2023.2231715

Madushanka, T., Kumara, D. S., & Rathnaweera, A. A. (2024). SecureRights: A blockchain-powered trusted DRM framework for robust protection and asserting digital rights. *arXiv preprint arXiv:2403.06094*. https://doi.org/10.48550/arXiv.2403.06094

Messina, M., Eslami, M. H., & Castilla, J. C. (2025). The use of blockchain in organisations for sustainable development: a systematic literature review and bibliometric analysis. *International Journal of Production Research*, 63(14), 5043-5070.

Meth, M. (2019). Blockchain in libraries.

Meth, M. (2019). Chapter 4: Barriers and Challenges to Blockchain Implementation in Libraries. *Library Technology Reports*, 55(8), 20-21. https://journals.ala.org/index.php/ltr/article/view/7188/9797

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://assets.pubpub.org/d8wct41f/31611263538139.pdf

Ogedengbe, F. A., & Adelowotan, M. O. (2025). Revolutionising corporate governance: blockchain's transformative impact and potential. *Frontiers in Blockchain, 8*, 1654633.

Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, 9(4), 1972-1986.

Rahmanova, A. (2025). Evolution of libraries in the digital Era: redefining access, education, and cultural preservation. *Library Archive and Museum Research Journal*, 6(1), 23-38.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Sandhu, G. (2018, February). The role of academic libraries in the digital transformation of the universities. In *2018 5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services (ETTLIS)* (pp. 292-296). IEEE.

Singh, A. K., Ashok/Ali Siddiqui Kumar Singh (Zeesha), & Singh, S. (2024). *Recent advances in computational intelligence and cyber security*.

Singh, B. P. (2018). Digital Transformation of library services in the Mobile World: The future trends. *Publishing Technology and Future of Academia*, 335-49.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".

Tamilselvan, N. (2024). Blockchain-based digital rights management for enhanced content security in digital libraries. *International Journal of Blockchain Technology (IJBT)*, *2*(1), 1-8.

Tella, A., Amuda, H. O., & Ajani, Y. A. (2022). Relevance of blockchain technology and the management of libraries and archives in the 4IR. *Digital Library Perspectives*, *38*(4), 460-475. https://doi.org/10.1108/DLP-08-2021-0065

Tella, A., Amuda, H. O., & Ajani, Y. A. (2022). Relevance of blockchain technology and the management of libraries and archives in the 4IR. *Digital Library Perspectives, 38*(4), 460-475.

Trist, E. R. I. C., & Emery, F. R. E. D. (2015). Sociotechnical systems theory. In *Organizational Behavior 2* (pp. 169-194). Routledge.

Viji, C., Jagannathan, J., Rajkumar, N., Mohanraj, A., Nachiappan, B., & Kovilpillai, J. A. J. (2025). Leveraging blockchain technology to enhance library security. In *Enhancing security and regulations in libraries with blockchain technology* (pp. 181-200). IGI Global. http://doi:10.4018/979-8-3693-9616-2.ch009

Werthmuller, N. (2025). Blockchain applied to digital archives. https://sonar.ch/global/documents/333098

Xu, H., & Zhang, N. (2023). Privacy implications of blockchain systems: a data management perspective. *Organizational Cybersecurity Journal: Practice, Process and People, 3*(1), 71-79.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., ... & Rimba, P. (2017, April). A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE international conference on software architecture (ICSA)* (pp. 243-252). IEEE.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078.*

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). Ieee.