information

MDPI

Article

Library Systems and Digital-Rights Management: Towards a Blockchain-Based Solution for Enhanced Privacy and Security

Patrick Laboso [1], Martin Aruldoss [1], P. Thiyagarajan [1], T. Miranda Lakshmi [2] and Martin Wynn [3,*]

[1] School of Mathematics and Computer Sciences, Central University of Tamil Nadu, Thiruvarur 610005, India; patrickkipkorirlphd21@students.cutn.ac.in (P.L.); martin@cutn.ac.in (M.A.); thiyagu@cutn.ac.in (P.T.)
[2] St. Joseph's College of Arts and Science (Autonomous), Cuddalore 607001, India; miranda@sjctnc.edu.in
[3] School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham GL502RH, UK
* Correspondence: mwynn@glos.ac.uk

Abstract

The rapid digitization of library resources has intensified the need for robust digital-rights management (DRM) mechanisms to safeguard copyright, control access, and preserve user privacy. Conventional DRM approaches are often centralized, prone to single-point-of-failure, and are limited in transparency and interoperability. To address these challenges, this article puts forward a decentralized DRM framework for library systems by leveraging blockchain technology and decentralized DRM-key mechanisms. An integrative review of the available research literature provides an analysis of current blockchain-based DRM library systems, their limitations, and associated challenges. To address these issues, a controlled experiment is set up to implement and evaluate a possible solution. In the proposed model, digital content is encrypted and stored in the Inter-Planetary File System (IPFS), while blockchain smart contracts manage the generation, distribution, and validation of DRM-keys that regulate user-access rights. This approach ensures immutability, transparency, and fine-grained access control without reliance on centralized authorities. Security is enhanced through cryptographic techniques for authentication. The model not only mitigates issues of piracy, unauthorized redistribution, and vendor lock-in, but also provides a scalable and interoperable solution for modern digital libraries. The findings demonstrate how blockchain-enabled DRM-keys can enhance trust, accountability, and efficiency through the development of secure, decentralized, and user-centric digital library systems, which will be of interest to practitioners charged with library IT technology management and to researchers in the wider field of blockchain applications in organizations.

Keywords: library management systems; digital rights management; DRM; blockchain; smart contracts; security; data privacy; Inter-Planetary File System; IPFS

Academic Editor: Aneta Poniszewska-Maranda

Received: 12 December 2025
Revised: 20 January 2026
Accepted: 27 January 2026
Published: 1 February 2026

1. Introduction

Digital libraries have transformed access to knowledge, enabling the global dissemination of e-books, journals, and multimedia resources [1]. With increased availability of e-books, digital journals, multimedia resources, and open-access repositories, libraries have shifted from being mere custodians of physical collections to becoming digital content providers for a global audience [2]. This shift, however, has introduced new challenges in the management of intellectual property and user-access rights [3], exacerbated by the growing use of Artificial Intelligence in literature generation and artistic creation [4]. Traditional digital library systems rely on centralized digital-rights management (DRM)

frameworks, which can be vulnerable to single-point-of-failure weaknesses, susceptible to unauthorized access, and be inefficient in the tracking of intellectual-property rights [3]. These limitations often lead to content piracy and erode trust among content publishers, libraries, and users. As digital-content consumption grows, there is an urgent need for secure, transparent, and decentralized solutions to manage digital assets effectively [5].

Blockchain technology, with its decentralized, immutable, and transparent ledger, offers a promising foundation for addressing these challenges [6,7]. By leveraging smart contracts and cryptographic mechanisms, blockchain enables secure peer-to-peer interactions without intermediaries, making it ideal for reimagining library systems [8–10]. Recent advancements in blockchain-based DRM have explored applications in music and image licensing, yet library-specific solutions remain underexplored, particularly in integrating robust key management for secure content access [11,12].

In this context, this article addresses the following research questions (RQs):

RQ1. What are the key challenges and available solutions for the deployment of DRM for library management systems?

RQ2. Can a decentralized DRM framework be designed and implemented for digital library management systems that uses blockchain technology and enhances security and privacy through advanced cryptographic techniques?

The rest of the article is structured as follows. Section 2 sets out the two phases of the research process, each with distinct methodologies and techniques. Section 3 then addresses the two RQs, setting out the findings from the integrative literature review and the controlled experiment. Section 4 assesses the performance and evaluation of the proposed solution. Finally, Section 5 concludes the paper, summarizing the main contribution, highlighting limitations, and pointing out possible areas for future research in this field of study.

2. Materials and Methods

There were two main phases to the research process (Figure 1). In phase 1, an interpretivist philosophy underpinned a qualitative assessment of the relevant literature from which a provisional conceptual framework (PCF) was developed as a basis for the design of phase 2. This approach is particularly appropriate for exploratory research when the researchers are looking to find an explanation of the phenomenon under study [13]. In phase 2, a positivist philosophy was adopted in a controlled experiment aimed at testing and verifying a decentralized DRM solution for digital library systems using blockchain technology. The two phases are discussed in more detail below.

2.1. Integrative Literature Review

Phase 1 comprised an integrative review of the relevant literature to identify key themes which could provide the basis for the PCF to guide phase 2 of the research. An integrative review allows for more open and flexible research and analysis compared to a systematic literature review. A range of search strings was used to find appropriate material available on the Internet between June and October 2025, using a combination of key themes derived from the RQs—"blockchain", "digital rights management", "DRM", "digital library systems", "cryptographic techniques", "challenges", "solutions", and variations on these main themes. From the initial location of relevant sources, other references were pursued and assessed in a snowballing process. Bell et al. [14] noted that such an approach "may be more suitable for qualitative or inductive researchers, whose research strategies are based on an interpretative epistemology" (p. 97).

This facilitated the mapping of the key concepts within the area of study and identification of the types of evidence that are available. It was a "broad scan of contextual literature"

through which "topical relationships, research trends, and complementary capabilities can be discovered" [15] (p. 351). Snyder [16] (p. 335) notes that "for newly emerging topics, the purpose [of an integrative review] is rather to create initial or preliminary conceptualizations and theoretical models, rather than review old models. This type of review often requires a more creative collection of data, as the purpose is usually not to cover all articles ever published on the topic but rather to combine perspectives and insights from different fields or research traditions". This can be used as the basis for developing a PCF, which Levering [17] notes is a good starting point to explain and examine a wider subject area.

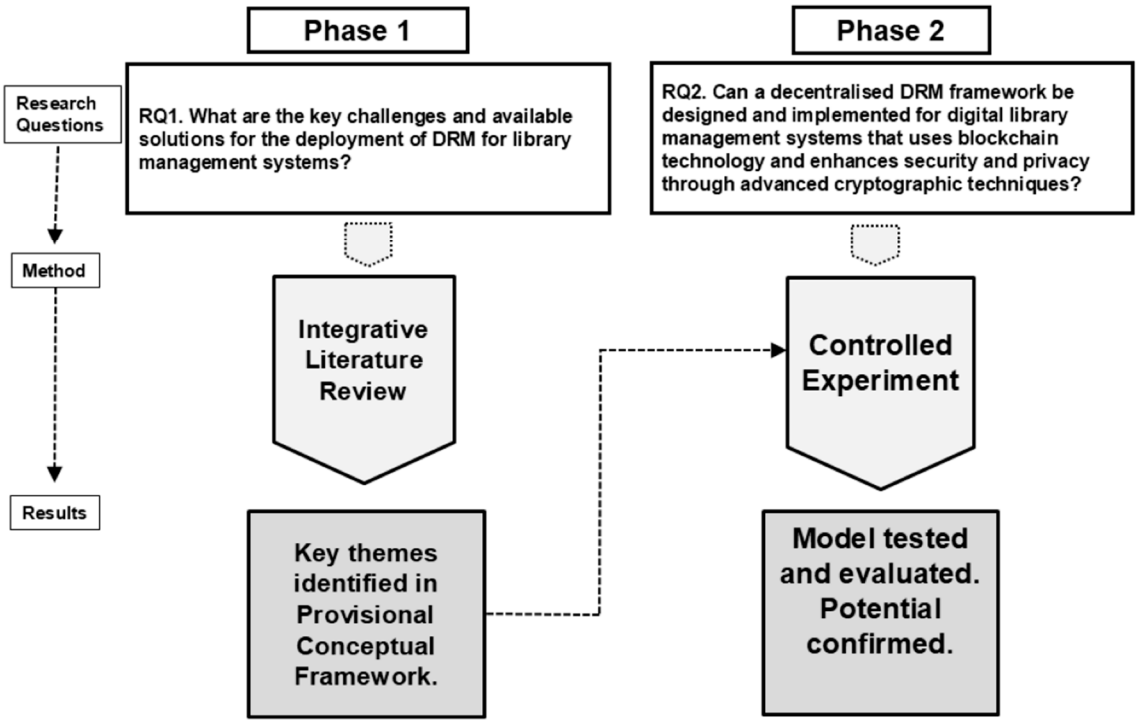

Figure 1. The two-phase research process.

Rocco and Plakhotnik [18] point out that there is no universally accepted definition of "conceptual framework" and that it is often used interchangeably with other terms like "theoretical framework". Jabareen [19], however, defines conceptual framework as "a network [. . .] of interlinked concepts that together provide comprehensive understanding of a phenomenon or phenomena". Merriam and Simpson [20] observe that it is normally grounded in a preceding literature review and represents the researcher's map of the area being investigated. Whilst concrete models may have precise variables and unambiguous parameters, the PCF instead provides an initial understanding and conceptualization of the subject under study [19].

2.2. Controlled Experiment

Phase 2 focused on the experimental development and implementation of a blockchain-based DRM library system, incorporating advanced cryptographic techniques to enhance data security and privacy. Such experiments can be seen as "a method of gathering information and data on a subject through observation in controlled settings" [21] (para. 1). The research adopts a simulation-based design to evaluate the proposed framework, an approach chosen because it allows for controlled testing of decentralized systems in a reproducible environment. This allowed the assessment of performance metrics like latency and throughput without deploying to a live, large-scale library network, which could be resource-intensive and risky during development. This approach is justified by the

need to simulate real-world library scenarios, for example, during peak-hour borrowing, where blockchain consensus and cryptographic operations introduce variables not easily captured in mere theoretical models alone. The strategy for evaluation scenarios involved stratified sampling: 100 simulated transactions per category (borrowing, reading, and returning), drawn from a pool of 500 users representing diverse roles (patrons, publishers, administrators). Scenarios were varied by network size (5–50 nodes) and load (low: 10 TPS; high: 300 TPS) to ensure representativeness.

This study adopts a hybrid experimental methodology that combines real blockchain deployment with controlled simulation-based evaluation. The real-world feasibility and correctness of the proposed blockchain-based digital library system are validated through deployment on the Ethereum sepolia test network, while scalability, network behavior, and security resilience under adversarial conditions are analyzed using the BlockSim simulation framework. Simulation parameter configurations are selected based on empirical Ethereum network characteristics, the existing blockchain literature, and the operational requirements of digital library systems. They include the number of nodes: Configured between 50 and 500 to represent medium- to large-scale blockchain developments; Block generation time: set to align with Ethereum's average Proof-of-Stake block interval; Transaction arrival rate: modeled using a Poisson distribution to reflect realistic user-access patterns in digital library environments; Network latency: configured across low- and high latency ranges to simulate geographically distributed nodes; Malicious node ratio: varied from 10% to 50% to evaluate security thresholds, including Byzantine fault tolerance limits and majority attack scenarios; Block and transaction size: derived from typical Ethereum smart contact interaction characteristics. This dual approach ensures both practical validity and rigorous performance evaluation.

At this stage, deployment and large-scale trials on a public mainnet are proposed as part of the future work when financial and operational constraints allow. Consequently, the current evaluation is based on simulation-based experiments, which allow controlled analysis of system behavior and performance. While these results provide meaningful insights into the feasibility and effectiveness of the proposed approach, we acknowledge that simulation outcomes may not fully replicate real-world mainnet conditions.

The proposed system is designed as a public blockchain network using the Ethereum platform, with evaluation conducted on the Sepolia testnet. Consensus uses Ethereum's Proof-of-Stake (PoS) consensus mechanism for efficiency and scalability on the public network. Key entities in the architecture include the following (Figure 2):

- Library Nodes: The blockchain nodes operated by participating libraries, responsible for validating transactions, and storing asset metadata. Furthermore, this layer serves as the policy enforcement and logging mechanism. Smart contracts are deployed on Ethereum to automate content licensing, manage DRM-keys, verify user-access rights, and ensure immutability of records. By using blockchain, the system eliminates reliance on a central DRM authority, reducing risks of manipulation, downtime, and single-point failures.
- Patrons: This is the term often used for end-users of library systems, these being students, researchers, and faculty members who access digital content via a client application (DApp). Patrons interact with the blockchain through wallets that manage their cryptographic keys.
- Publishers: Authors or publishers are individuals who upload digital assets (e-books, journals) and define initial access policies.
- Off-Chain Storage: Decentralized storage solutions include using IPFS for storing encrypted digital content, with hashes referenced on the blockchain to ensure integrity. Storing digital content directly on the blockchain is costly and inefficient due to

block-size limitations. Therefore, the Inter-Planetary File System is employed to store encrypted versions of digital resources. IPFS is a distributed, peer-to-peer storage network that identifies content by a content-addressable hash [22]. This ensures that even if a file is moved or duplicated across the network, it can still be uniquely verified and retrieved.

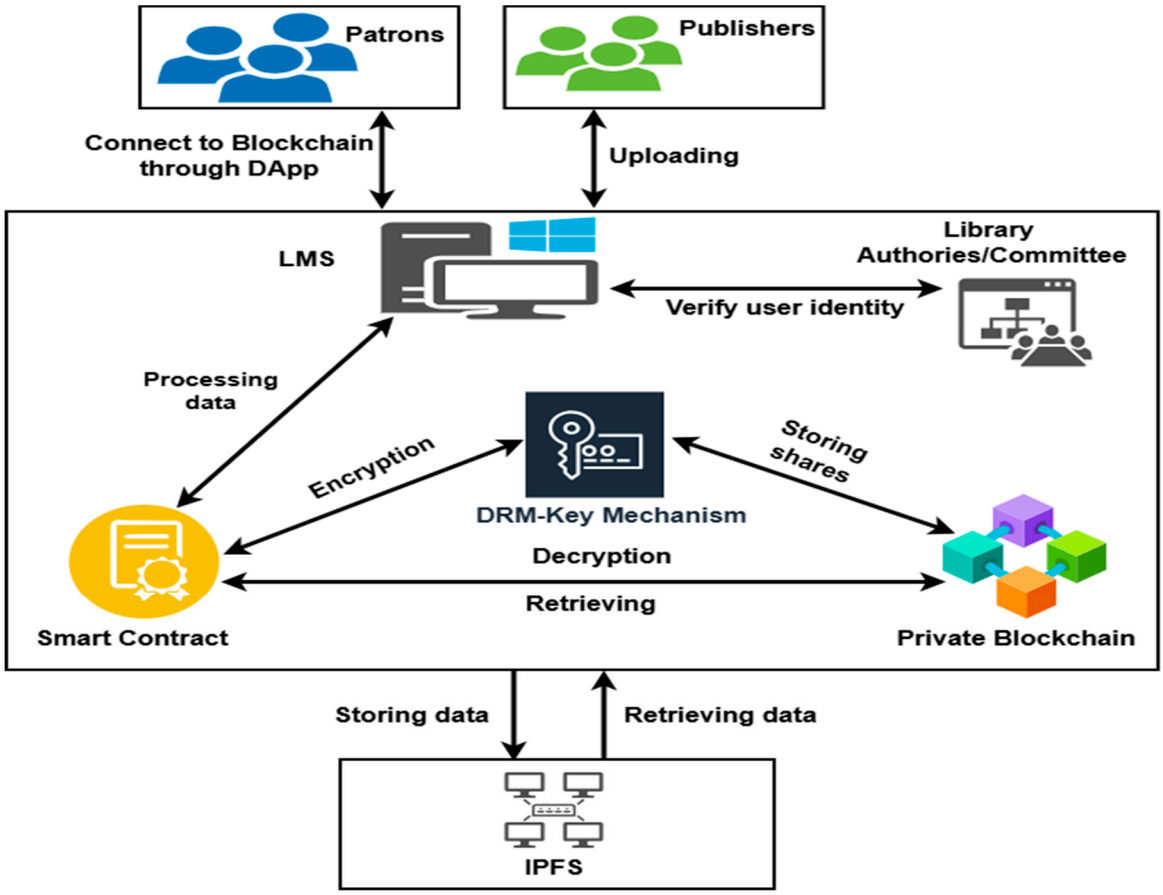

Figure 2. The blockchain-based library management system (LMS) architecture used in the controlled experiment.

In a blockchain-based library management system, the user-side typically refers to a decentralized application (DApp) that allows patrons to browse, borrow, return, or propose books via a web- or mobile interface connected to their crypto wallet (MetaMask). The library side represents the administrative backend or interface used by librarians or institutions to manage inventory, approve transactions, track holdings, and enforce policies. Since these systems leverage blockchains for transparency, immutability, and decentralization, the blockchain can be viewed as the core mediator.

Both sides interact with the same smart contracts deployed on a blockchain network (Ethereum). The DApp (user side) sends transactions to invoke contract functions, such as borrowing a book (which might transfer a digital token representing the book). The library side monitors blockchain events or queries the contract state to verify and respond (approving a loan or updating availability). This ensures all actions are recorded on-chain, preventing disputes over due dates, ownership, or fines.

The validation methodology went beyond deployment to include functional testing like end-to-end borrowing cycles, security audits using tools like Mythril for smart contracts, and comparative analysis against baselines. The comparative baseline is explicitly defined as (1) a centralized DRM system (Adobe Content Server simulation with single-

server key management), and (2) a Basic Blockchain DRM (Ethereum with on-chain key storage without secret sharing). Metrics were collected over 30 simulation runs per configuration, with statistical significance tested via t-tests ($p < 0.05$) for differences in latency and throughput.

3. Results

3.1. RQ1: What Are the Key Challenges and Available Solutions for the Deployment of DRM for Library Management Systems?

DRM systems have traditionally been employed to enforce copyright, regulate access, and protect digital content from unauthorized usage. Despite their widespread adoption, conventional DRM approaches are largely centralized and are often controlled by publishers or service providers, thereby introducing significant concerns regarding transparency, interoperability, and user privacy. As such, centralized DRM systems face multiple limitations. First, the reliance on a single authority or vendor creates a single-point-of-failure, making the system vulnerable to attacks, outages, or misuse of authority [23]. Moreover, centralized DRM mechanisms often restrict interoperability across different platforms, leading to vendor lock-in and reduced accessibility for users. Furthermore, centralized control of access keys and licenses compromises user privacy, as sensitive information is stored and processed in a manner that can be tracked or exploited by third parties. These drawbacks highlight the need for alternative DRM solutions that are not only secure and efficient but also decentralized, transparent, and privacy-preserving.

Blockchain technology has emerged as a promising enabler of decentralized access control and digital-asset management [24]. Its inherent immutability, distributed consensus, and transparency make it suitable for addressing the shortcomings of centralized DRM [5]. By employing smart contracts, blockchain can automate license issuance, enforce access policies, and ensure accountability without reliance on a central authority [3]. When integrated with decentralized storage solutions such as the Inter-Planetary File System (IPFS), blockchain further enables the secure storage and retrieval of digital content in a distributed manner, reducing the risks of censorship, data loss, and single-point vulnerabilities. IPFS is used to store metadata, reducing the handling of bulk, content-heavy data on the blockchain system, while blockchain records and stores hashes. Storing hashes on a blockchain rather than a conventional centralized server is justified by the need for unbreakable trust and permanence in a system handling valuable intellectual property. Once a hash is recorded on the blockchain, it cannot be changed, unlike a traditional server-based storage system, where admins can modify entries. Blockchain eliminates the need for a trusted third party by ensuring validity through consensus among nodes. Additionally, blockchain provides a public, timestamped ledger of hashes, enabling easy dispute resolution, which traditional servers lack due to their lack of an inherent audit trail in the event of a hacked or damaged system. Indeed, the integration of blockchain technology into digital-rights management (DRM) systems has revolutionized the way intellectual property is protected and managed across various digital environments, including music, images, code, and other forms of media [25]. However, in library systems, minimal- or no tangible research has been conducted [26].

It is thus of relevance and value to review how blockchain has been deployed to address the challenges in DRM in other fields. To the best of our knowledge, this study is the first to propose a comprehensive and secure blockchain-based digital-rights management framework specifically designed for integration within library systems. These works offer valuable insights that can be applied to enhance blockchain-based library systems through decentralized DRM-key mechanisms. It is thus of relevance and value to review how blockchain has been deployed to address the challenges in DRM in other fields (Table 1).

For example, Tamilselvan, N.D. [27] proposes a blockchain-based DRM framework that replaces centralized control with a tamper-proof ledger and smart contracts, encoding access permissions, expiration dates, and usage conditions directly on the chain. The proposed system also integrates decentralized identity solutions (uPort) to provide users with secure, self-sovereign authentication while protecting their personal data. The proposed system is built on a permissioned Hyperledger Fabric. The system's smart contracts automate licensing, reducing administrative overhead and ensuring that content usage aligns precisely with rights, thereby improving efficiency and auditability. The system demonstrated a transparent and efficient digital-library ecosystem that extends beyond academia to broader digital-content distribution and copyright protection. In a similar vein, Mhsnhasan et al. [28] propose integrating Artificial Intelligence (AI) and blockchain technologies to enhance digital-rights management (DRM) systems in libraries, addressing challenges related to intellectual property protection, Central-point failure, access control, and operational efficiency. The proposed system is built on a hybrid framework that couples Artificial Intelligence (AI)-driven behavioral analytics, anomaly detection, and demand forecasting with blockchain's immutable ledger and smart-contract licensing. The system architecture comprises three layers: an AI-based access-management module, a blockchain infrastructure that records transactions and enforces smart contracts, and an interoperability module for integration with existing library systems. A novel Content Access Integrity Score (CAIS) aggregates blockchain transaction consistency, AI anomaly scores, and license validity to produce a trust metric for each access request. The performance evaluation demonstrated that the hybrid model achieves a prediction accuracy of 95%, which is significantly higher than the 81.2% achieved by the traditional rule-based DRM. Moreover, unauthorized access attempts drop by an average 38% when AI is incorporated.

Table 1. Articles related to DRM and blockchain in other research fields.

Domain	Blockchain Platform	Challenges Identified	Key Finding/Outcomes
Digital-rights management [27]	Hyperledger Fabric (permissioned blockchain).	Traditional DRM systems are vulnerable to piracy and illegal content sharing, making it difficult to fully secure digital assets. Existing systems struggle to balance strong authentication with user privacy, often exposing personal data to risks. Licensing agreements are often cumbersome, slow, and administratively heavy, leading to delays and inefficiencies in content distribution.	Reduced licensing delays and administrative costs. Encourages fair use and sharing while protecting creators' rights. Builds trust among stakeholders due Higher throughput and lower latency compared to traditional DRM. The system is efficient, secure, and feasible for real-world deployment.
Digital-rights management [28].	Hybrid system.	A single-point of control architecture. Lacks verifiable audit trails. Relies heavily on machine for licensing and content management.	Streamlined rights enforcements, licensing, and access control. Build trust among authors, publishers, and users, ensuring fair use and reducing piracy. Secure and transparent access to digital resources. Reduces disputes over ownership and licensing.
Educational Technology—MOOCs, Online Learning [29].	Hybrid Architecture: Public blockchain (digital certification) + Private blockchains (resource rights management).	Infringement of digital copyrights of multimedia learning resources. Insecurity of digital education certificates (vulnerable to theft, tampering, forgery). Low degree of openness—isolated islands of educational datasets. Declining credibility of Certificate Authority (CA) ecosystem. Lack of unified evaluation standards for e-learning.	Three-network architecture: Learning User Network (LUN), Education Certification Network (ECN), Multimedia Educational Resource Local Networks (MERLNs). Dual blockchain types: MDR Private Blockchains for resource rights, DC Public Blockchain for certificates. Unmediated certificate verification using public key cryptography. Scalable to support diverse educational functions while maintaining security.

Table 1. *Cont.*

Domain	Blockchain Platform	Challenges Identified	Key Finding/Outcomes
Digital copyright protection [30].	Private blockchain network with IPFS.	Ensuring watermarks remain intact under transformations (compression, resizing, cropping, filtering). Current system produce false positives or negatives under certain image manipulations. As more content is registered, blockchain-size grows, raising concerns about transaction speed, cost, and long-term sustainability.	Embedding QR codes via DCT-based watermarking proved resilient against common manipulation (compression, resizing, cropping, and filtering). A trusted environment for digital-content distribution, where ownership and authenticity can be independently verified. The system successfully asserts ownership and prevents piracy.
Digital copyright protection in education resources [31].	Hyperledger Fabric.	Easy duplication and dissemination of resources. Copyright infringement risks. Lack of multidimensional copyright evidence. Weak infringement-tracking mechanisms.	Security improvement by ensuring data integrity, guaranteeing authenticity, and providing immutability. Privacy protection through RSA encryption of identity. Showed high perceived usefulness, ease of use, and willingness to use. The system encourages creativity and resource sharing.
Digital copyright protection [32].	Ethereum blockchain.	Current systems lack mechanisms for effective sharing of physical books across institutions, resulting in low utilization rates. Each university traditionally develops its own independent library management software, leading to duplication of effort, wasted resources, and high cumulative costs.	Efficient resource utilization. Tamper-proof records of borrowing and returning. Cost reduction.
Digital-rights management (multimedia content) [33].	Scalable blockchain with overlay network with pBFT consensus.	Current DRMs are unable to trace who should be responsible for violations. There is a need for a new DRM framework that is reliable, efficient, tamper-resistant, and secure. Core issue is the scalability of blockchain. Digital content that becomes easily available will in time be worthless. No way to track the leakage or copyright for spread of digital material.	Proposed overlay network with cluster heads (CH) to improve throughput. DCT-based watermarking with SPECK lightweight encryption. Achieved improved scalability: blocks propagated in t_hop instead of 8t_hop. Cloud storage for multimedia with blockchain for metadata.
Copyrights management [34].	Private blockchain (JAVA-based) with POW.	Massive open-source projects making copyright registration difficult. Lack of unified copyright-management platform. Decentralized copyright resource and vague copyright ownership.	Achieved accuracy meeting verification requirements. Code fingerprint (256-bit hash) provided best storage efficiency. Better response speed and storage efficiency. Verification model handles code plagiarism effectively.

In the field of online education, Guo et al. [29] designed a blockchain-enabled DRM-system tailored for multimedia resources. It introduces a novel network architecture that combines public- and private blockchains, along with three specific smart-contract schemes, to effectively record digital rights, securely store certificates, and enable unmediated verification of digital certificates. The system aims to enhance security, transparency, and openness in managing online educational multimedia content while facilitating the creation of lifelong-learning passports. The proposed approach offers a promising solution for protecting multimedia resources and certificates in online-education environments, leveraging blockchain's decentralized and tamper-proof features. Additionally, Chen [30] proposed a blockchain-based open-service platform for university digital-resource systems to overcome the limited openness, cumbersome copyright certification, and security weaknesses of current systems. The proposed system leverages blockchain's distributed ledger, immutability, transparency, and decentralization to ensure data integrity, protect user-privacy through encryption, and provide traceable, tamper-proof records of educational resources. The sys-

tem architecture adopts a consortium model, where each university department operates a private chain for teachers and students. An alliance (consortium) chain interconnects these private chains to enable cross-campus sharing via a high-speed P2P network. Uploaded resources are automatically reviewed by smart contracts and authenticated through consensus mechanisms, PoS, guaranteeing impartiality and fairness. Moreover, the platform incorporates an incentive system that awards virtual-currency based on publishing activity, views, and downloads, motivating continuous contributions. The performance evaluation of the system demonstrates that the proposed design improves resource utilization, promotes educational equity, and accelerates the digital transformation of higher education through a secure, efficient, and transparent blockchain-enabled ecosystem.

Zhao et al. [31] proposed BC-DERCP, a blockchain-based mechanism to protect the copyright of digital educational resources (DERs), which are easily duplicated and disseminated online. Leveraging a consortium Hyperledger Fabric network, the system stores only essential metadata (encrypted user identity, perceptual hash, digital signature, timestamp) on-chain. At the same time, the full resources and watermarked copies remain off-chain, thereby reducing redundancy and preserving privacy. They implemented three smart contracts for user-information registration with RSA encryption, resource-copyright storage that records a SHA-256 hash, ECDSA signature, and perceptual hash, and copyright-infringement verification via watermark extraction and hash comparison. This secure-storage workflow combines encryption, DCT-based digital watermarking, and perceptual hashing to generate multidimensional copyright evidence. Experimental evaluation demonstrates a 100% transaction success rate with minimal latency, showing that a consortium blockchain can provide tamper-resistant, privacy-preserving, and verifiable copyright protection for educational digital assets.

Liu [32] proposed a university book-sharing cloud platform that integrates blockchain and cloud computing to enable cross-regional, cross-university borrowing of books. Traditional universities suffer from duplicated infrastructure and low-utilization of paper books, while courier services can support remote borrowing but lack a coordinating platform. The proposed system adopts a six-layer logical architecture built on a consortium blockchain (Ethereum) delivered via Blockchain-as-a-Service, leveraging cloud computing's virtualization and scalability. In the system, the improved Delegated Proof-of-Stake mechanism selects delegated nodes based on multidimensional participation metrics to achieve fast, second-level consensus while mitigating negative voting. The performance evaluation demonstrates that breaking geographical barriers, reducing duplicate construction costs, improving book-use efficiency, and providing a secure, non-tamperable environment for university libraries is possible.

Yuan et al. [33] similarly integrated blockchain technology with zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) and trusted execution environments (TEEs) in a comprehensive scheme for secure IoT data sharing. The proposed system addresses critical security and privacy challenges in IoT systems, including user anonymity, identity unforgeability, and secure key transmission. This approach involves constructing anonymous credentials using zk-SNARKs and blind signatures, implementing a multi-hop proxy re-encryption mechanism for secure data transmission without interaction, and utilizing a TEE blockchain to ensure data confidentiality, integrity, and access control. Security and performance analyses demonstrate that the scheme effectively safeguards user privacy, resists forgery, and ensures efficient data exchange, making it applicable for secure IoT data-sharing scenarios. In copyright management, Jing et al. [27] proposed a blockchain-based code copyright management system that functions by verifying the originality of uploaded code using an Abstract Syntax Tree (AST)-based similarity model and storing copyright information on a Peer-to-Peer blockchain network. This

system addresses rampant code plagiarism in open-source software projects by enabling traceable and tamper-proof copyright records, ensuring that original code is protected from unauthorized use and misuse. Its importance lies in providing a fundamental solution to copyright confirmation beyond mere detection, making it highly useful for developers and organizations in maintaining the integrity of intellectual property in collaborative software environments.

In summary, despite some progress in the development of blockchain-based library systems, a critical gap remains in effectively managing digital- and intellectual-property rights associated with digital resources. Figure 3 depicts the PCF for the controlled experiment, illustrating the main challenges and potential benefits of adopting a blockchain-based solution. Existing approaches primarily focus on secure data-storage and transaction transparency but lack comprehensive mechanisms for enforcing ownership, usage control, privacy, and rights protection. Examples from the literature in related and other fields underline the potential of a blockchain-driven decentralized library system that integrates a DRM key mechanism with other technologies, utilizing smart contracts and cryptographic operations, for a more secure, transparent, and intermediary-free access to digital assets, while preserving ownership rights and access integrity (Table 2). Based on these technologies, a secure digital-rights library management system can protect intellectual property, ensuring trustworthy access control and preserving the integrity of the digital library collection. Incorporating these layers (Figure 3) forms the foundation for strong content protection. Each layer serves a distinct function, ensuring confidence in the protection of every digital object.

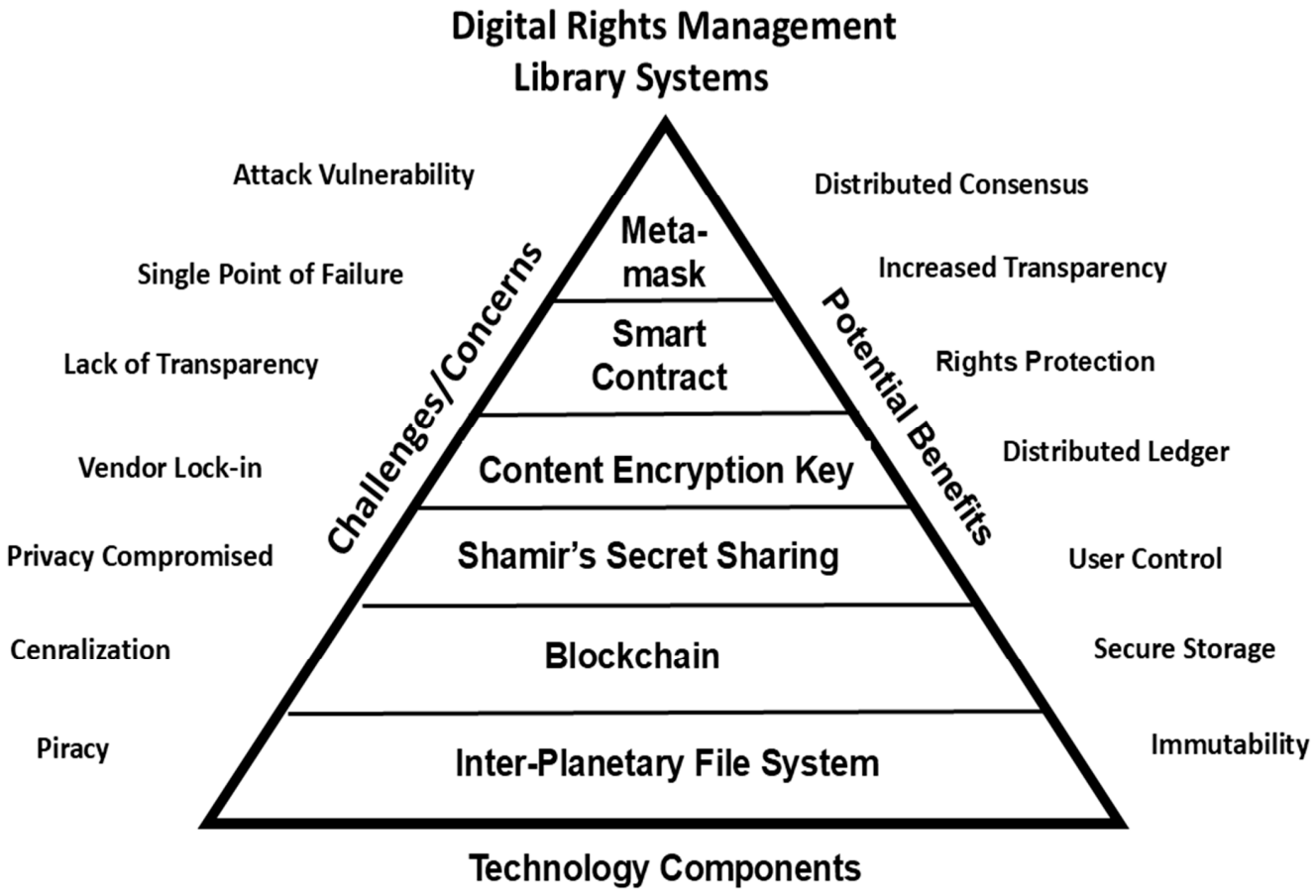

Figure 3. Provisional conceptual framework: challenges, potential benefits, and technology components.

Table 2. Technology components of digital-rights management system.

Technology Layer	Technology Description/Function
Meta-mask	A digital wallet that manages the interaction between the patron and the library system. The meta-mask provides a wallet-based authentication. Each patron has a unique wallet address that serves as the user's identity.
Smart Contract	Provides a set of automated, transparent, and trustworthy rules that enforce agreements when predetermined conditions are met.
Content Encryption Key	An encryption and decryption stage for digital content. Symmetric cryptographic keys, such as AES-128 or AES-256, are used for encrypting and decrypting content.
Shamir's Secret Sharing	A layer that provides a method to split the Content Encryption Key (secret Keys) into multiple shares securely and distribute the created shares among participants. The reconstruction requires a threshold number of shares, usually a minimum of three, to acquire the original secret key.
Blockchain	A distributed digital ledger that records every single transaction in a block. Each new block is cryptographically linked to the previous block, forming a chain of blocks that is secure and immutable. The addition of new records to the blocks is achieved through consensus mechanisms.
Inter-Planetary File System	A peer-to-peer network for storing large amounts of metadata and sharing files in a distributed manner. The acquisition of files from the IPFS is based on content addressing.

3.2. RQ2: Can a Decentralized DRM Framework Be Designed and Implemented for Digital Library Management Systems That Uses Blockchain Technology and Enhances Security and Privacy Through Advanced Cryptographic Techniques?

A blockchain-based decentralized library management system was implemented on the Ethereum blockchain, a public, permissionless platform. The framework leverages smart contracts to manage key operations within a library ecosystem's decentralized applications (dApps). These operations include user registration, digital-wallet generation, library-resource tokenization, digital-asset verification, and content distribution as outlined in Section 2. The proposed solution incorporates decentralized DRM-key mechanisms designed to secure digital content distribution and access. Central to this approach is the use of Content Encryption Keys (CEKs), which is a symmetric key for both encryption and decryption, used for digital assets such as e-books, to prevent unauthorized access. To enhance the security and resilience of the CEKs, Shamir's Secret Sharing is employed to distribute CEKs across multiple stakeholders' nodes, ensuring that no single entity holds the complete key, thereby mitigating risks of key compromise [35]. Smart contracts automate key issuance, access control, and revocation.

The proposed system is deliberately designed for the unforgiving reality of public blockchains: adversaries range from curious insiders (semi-honest library nodes) to outright malicious outsiders capable of transaction forgery, replay attacks, denial-of-service floods, and sophisticated social-engineering. Quantum threats are not an afterthought, but a primary concern, with built-in migration paths to NIST-approved post-quantum signatures, such as Dilithium [36,37]. Patron privacy is protected through ε-differential privacy ($\varepsilon = 0.05$) noise injection and pseudonymous wallet interactions, ensuring reading habits remain untraceable even on Ethereum's transparent ledger while fully complying with GDPR without compromising auditability [38,39]. To enhance user privacy in the decentralized library system, ε—differential privacy (DP) is employed with $\varepsilon = 0.05$, a strong privacy parameter that bounds the risk of identifying individual borrowing activities while allowing useful aggregate insights [40]. Differential privacy ensures that the output of a query on borrowing records such as transaction logs containing user IDs, book CIDs, and timestamps changes minimally when any single record is added or removed, thus protect-

ing against inference attacks. The focus is on the Laplace mechanism, which adds calibrated noise to query outputs and is suitable for numeric aggregates like borrowing counts [41,42].

The Inter-Planetary File System (IPFS) is integrated within the system to manage and store large data materials [43,44]. In the proposed solution, the publisher uploads the digital content, such as an e-book or journal, to the library system. The digital content is then encrypted, and metadata is stored on IPFS. The IPFS distributes the content across its decentralized network, breaking it into chunks and assigning a unique Content Identifier (CID), a cryptographic hash that serves as the content's address [45,46]. The CID ensures content integrity and retrievability. The content is encrypted before storage to enforce DRM, with encryption keys managed separately. The CID is then submitted to a smart contract on the Ethereum blockchain. The smart contract records the CID as a transaction, which undergoes consensus validation by network nodes [47]. Once validated, the transaction, including the CID, is stored on the blockchain ledger, creating an immutable record. The full content remains on IPFS for efficient storage, while the blockchain only stores the CID, enabling verification and access [48]. This dual approach optimizes security, scalability, and auditability for digital-rights management. The mechanism integrates blockchain technology with advanced cryptographic techniques to provide secure, transparent, and scalable management of digital assets. By decentralizing key distribution and access control, the system addresses limitations in traditional DRM, such as centralized vulnerabilities and privacy concerns.

The implementation utilizes the Remix IDE, Solidity programming language, and MetaMask wallet to develop blockchain solutions on the Ethereum platform and deploy on the Sepolia test network for realistic evaluation of the smart-contract execution, transaction costs, and state transitions without incurring real financial cost. Remix IDE provides a robust development environment tailored for Ethereum smart-contract deployment, while Solidity is used to write the smart-contract code. The MetaMask wallet secures transactions within the peer-to-peer library network. For decentralized storage, the Inter-Planetary File System (IPFS) was employed. In addition, the system's security and performance evaluation was conducted on the Blocksim framework enabling controlled modeling of the blockchain network by allowing customization of the network size, consensus behavior, transaction arrival rates, and security resilience under adversarial attacks.

In the proposed system, digital content is not encrypted within the library system by the publisher to ensure standardized security before being stored on IPFS and tracked via blockchain (Figure 4). The CEK ensures that only authorized users verified via blockchain smart contracts can access the original content. AES-256 in GCM mode is used as the encryption algorithm, providing authenticated encryption with 256-bit keys for efficiency, security, and integrity checks against tampering.

When a publisher uploads digital content to the library system, a unique CEK is generated specifically for that content using a cryptographically secure pseudo-random number generator (CSPRNG) from the operating system's entropy pool. This ensures that each piece of IP has its own isolated security. The CEK is a 256-bit random string. Reusing keys across contents could lead to widespread compromises if one key is exposed. Uniqueness prevents this and ties the key to the content's blockchain metadata.

The original digital content plaintext is denoted as P and is fed into an encryption algorithm along with the CEK, which is denoted as K. The algorithm transforms P into ciphertext C, which is unreadable without K. This ciphertext is then uploaded to IPFS, where it is stored, decentralized, and referenced by a Content Identifier (CID) on the blockchain. An Initialization Vector (IV) is generated randomly (96-bit for GCM) per encryption to ensure semantic security, preventing pattern analysis even for identical plaintexts. Details of the encryption/decryption Formulae are provided in Appendix A.

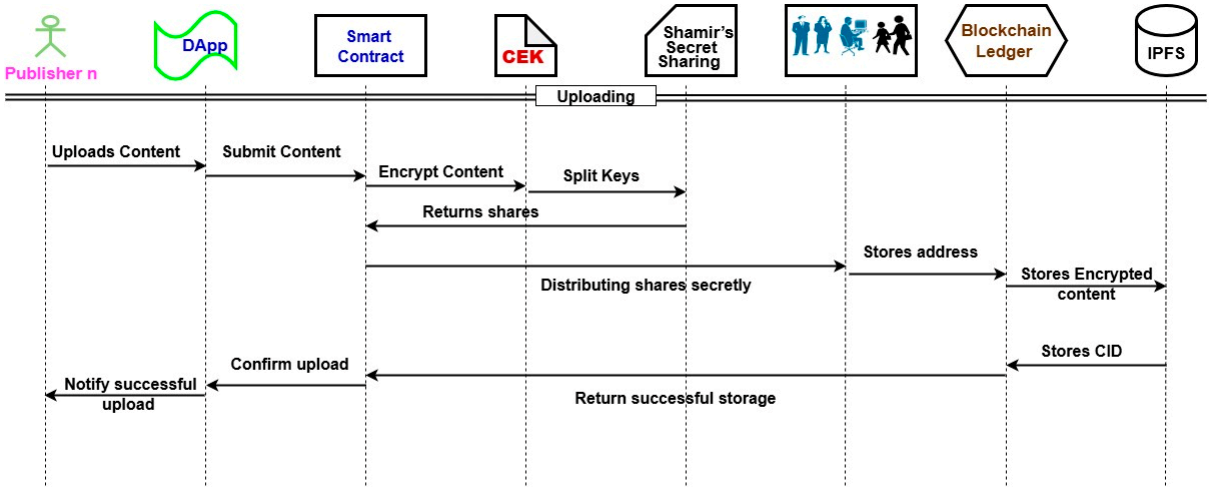

Figure 4. Uploading and encryption process in the proposed system.

Shamir's Secret Sharing (SSS) is deployed to split the CEK (S) into n = 5 shares with k = 3 threshold, where the minimum number of shares is required to reconstruct the original CEK (S) [49,50]. The smart contract automates the distribution of shares among different trusted parties within the system, eliminating the need for intermediaries to determine the share distribution. If fewer than k shares are available, an administrator override mechanism with audit logging is provided as a secure fallback option. Threshold security is ensured, as any group of k or more shares can reconstruct the CEK. Fewer than k shares reveal no information about the CEK due to the information-theoretic security of SSS. The system has flexibility in that it chooses k and n (where k $\leq n$) based on security- and access requirements. For this reason, the SSS is utilized in this system because it provides flexibility to model the threshold according to the requirements and capacity to scale accordingly, varying participant count and security, making it ideal for a decentralized system where centralized authority is undesirable. For example, if n = 5 and k = 3, five shares are distributed, but any three share are sufficient to recover the CEK. The shares are divided into five shares, each to be managed by a distinct entity, to balance trust, accountability, and redundancy. These entities correspond to key roles in the system architecture.

Secret s identifies the actual value being protected (the CEK), whilst the smart-contract component demonstrates how shares are distributed within the system. Publishers are intended to hold a share so that they can trace usage, reduce piracy, and prevent cheating after their content has been shared with the library. The process of share generation and the generation of the secret s (which represents the CEK) is further detailed (in two steps) in Appendix B (Shamir's Secret Sharing Foundations).

Key rotation is implemented to enhance cryptographic resilience and minimize long-term exposure of sensitive data. A new CEK is periodically generated every 90 days or immediately upon the detection of a potential compromise. Subsequently, all encrypted content is re-encrypted off-chain using the newly generated CEK to ensure efficiency and data consistency. The previous key shares, distributed through Shamir's Secret Sharing, are invalidated via a smart-contract burn operation to prevent unauthorized reconstruction of the old CEK. This process effectively mitigates prolonged key exposure and reduces the potential impact of compromised keys on the overall system security.

As regards digital acquisition, there are three main processes: borrowing, reading, and returning. The borrowing process begins when a registered patron selects an e-book or journal via the Library dApp, a user-friendly interface for blockchain interactions. The dApp submits a borrowing request to a smart contract on the Ethereum blockchain. The smart contract verifies the patron's eligibility by checking membership status, borrowing

tokens, e-book availability, and access-rights stored on IPFS. Upon verification, the smart contract receives an approval or denial notice as illustrated in Figure 5. If approved, the smart contract activates a Content Encryption Key (CEK) session in the DRM-key manager, collecting shares from at least three stakeholders; for example library administrators, one member, and the publishers to reconstruct the CEK using threshold cryptography. The smart contract then decrypts the IPFS-stored content and delivers it to the dApp for the patron to read. The transaction is submitted for blockchain consensus, with records stored on IPFS and the hash on the ledger, ensuring a secure and auditable process. If denied due to insufficient tokens or expired membership, the patron is notified via the dApp, and the denial transaction is recorded on the blockchain after consensus. The transaction details are stored on IPFS, with its hash on the blockchain ledger (Figure 5).

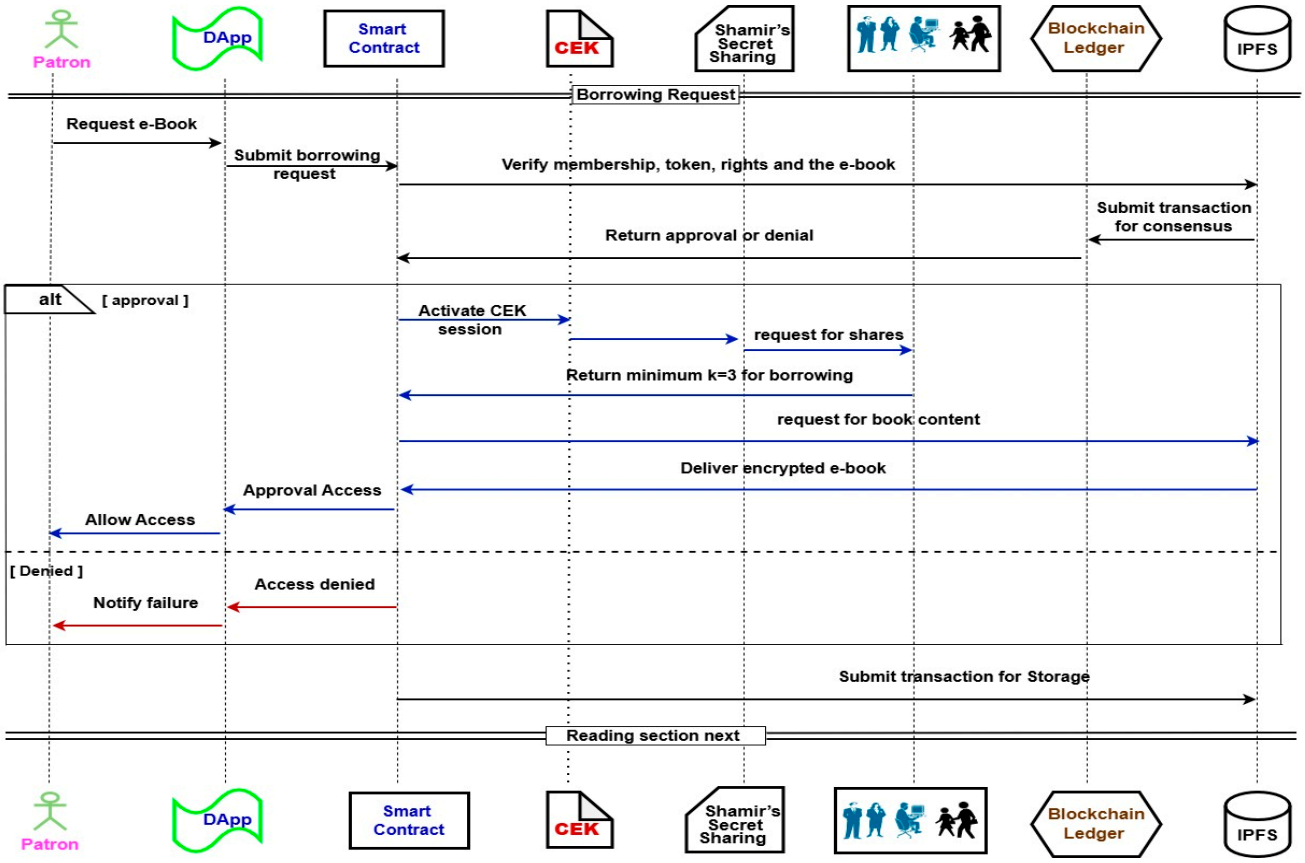

Figure 5. A sequence diagram illustrating the patron access procedure with DRM-key mechanisms.

The reading process allows patrons to access borrowed content through the Library dApp's reading interface, which supports features like annotations while enforcing DRM rules. To continue reading, the patron submits a reopen-access request via the dApp, triggering the smart contract to re-verify eligibility using IPFS records. This checks the loan period (14 days), usage limits like one-time access, or membership status. If eligible, the smart contract grants access, reactivating the CEK session, and the patron resumes reading in a secure viewer preventing unauthorized actions. The access event is recorded as a blockchain transaction, with details stored on IPFS and the hash on the ledger. If ineligible due to an expired loan or restricted access the patron is notified of the denial, access is revoked, and the termination transaction is logged on the blockchain and IPFS. This ensures dynamic rights enforcement and compliance with licensing terms.

The returning process concludes the patron's access to a borrowed e-book or journal. The patron submits a return request via the Library dApp, which the smart contract verifies

using IPFS records to confirm the asset's status. Upon validation, the smart contract revokes active CEK sessions, locking the content as illustrated in Figure 6. The return is recorded as a blockchain transaction after consensus, with details stored on IPFS and the hash on the ledger. The patron is notified of the successful return, often with borrowing summaries or recommendations. Automatic returns, triggered by loan expiration, follow a similar process, ensuring resources are quickly available for others. This efficient mechanism supports scalable resource management while maintaining security and transparency.

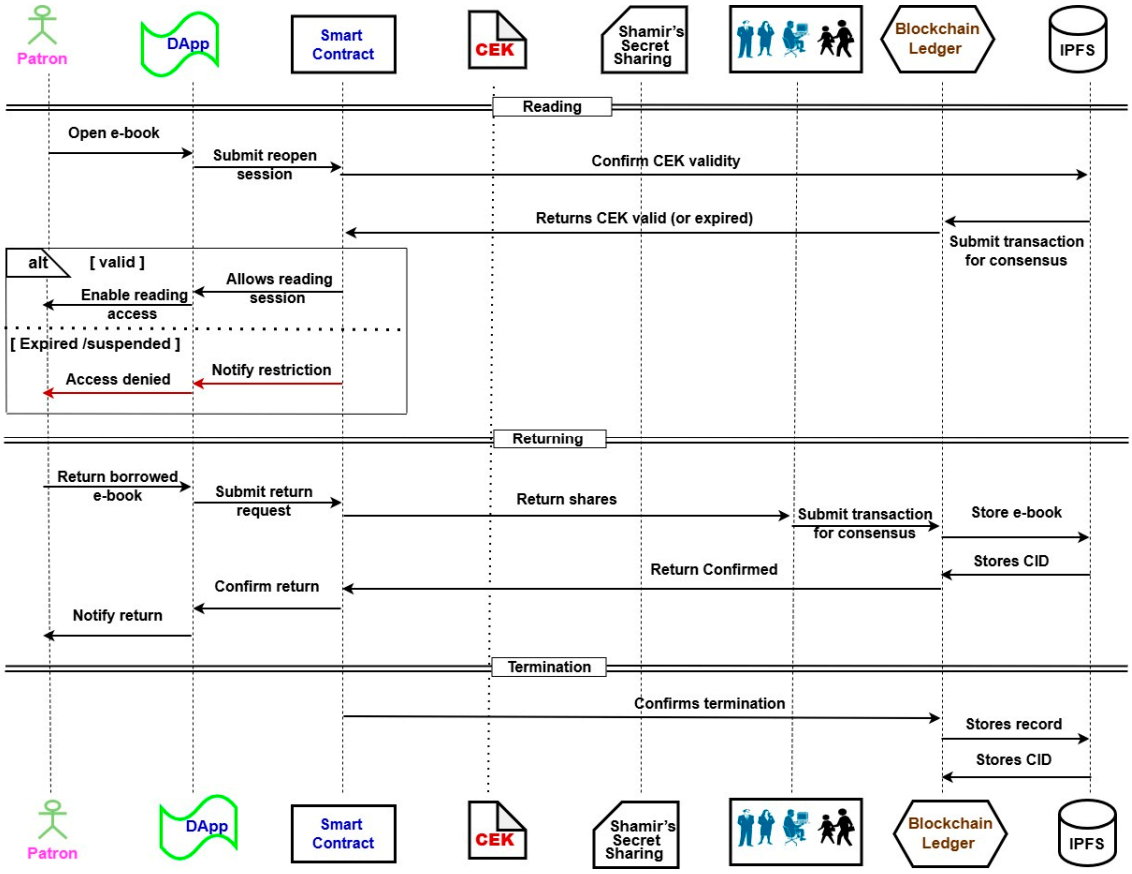

Figure 6. A sequence diagram illustrating the patron's reading and returning procedure with DRM-key mechanisms.

As an illustration in practice, consider student Alice is borrowing an e-book. Alice logs into the dApp, selects the book, and submits a request. The smart contract verifies her membership (valid) and tokens (sufficient), collects three shares (from publisher, admin, faculty), reconstructs the CEK, decrypts the content from IPFS, and streams it to Alice's viewer for 14 days. If Alice tries to copy, DRM enforces restrictions. Upon return, shares are invalidated and access is revoked.

Borrowing records are stored as immutable transactions on the blockchain via smart contracts logging events like borrowing requests. To prevent linkages such as inferring a user's reading habits from exact borrow counts, noise is injected during aggregate queries rather than raw record storage. This preserves the blockchain's mechanism, as it is simple, efficient for count queries, and achieves ε-DP [41].

4. System Performance and Evaluation

To evaluate the framework's performance, the BlockSim simulation toolkit [51] was used, focusing on key metrics: throughput, latency, response time, and standard deviation. BlockSim was configured with a full-mesh network topology, 20 nodes (simulating libraries),

block size of 1 MB, and Ethereum-like PoW consensus with 15 s block intervals. Simulations were ran 30 times per scenario, with stress-testing up to 500 concurrent users. These indicators provide insights into the system's effectiveness, scalability, and dependability, confirming its suitability for managing digital rights in library environments. Statistical significance was assessed using paired t-tests ($p < 0.01$) comparing to baselines.

4.1. Deployment Analysis

The proposed blockchain-based library digital-rights management (DRM) architecture is built and deployed on the Ethereum-distributed ledger platform. The experimental procedures are conducted on a Windows 11 (64-bit), equipped with an Intel core processor featuring four cores and 16 GB of memory. The implementation process begins with establishing the smart-contract (SC) infrastructure using the Meta-Mask digital-wallet interface. Figure 7 illustrates the successful setup, detailing key specifications such as contract address, nonce, sepolia amount, gas limit in units, gas used in units, base fee, total gas fee, max fee per gas, and the total transaction cost in Ether for the library DRM system. This deployment consumed an average of 1,200,000 gas (std dev: 50,000), 20% less than a Basic Blockchain DRM baseline due to optimized code.

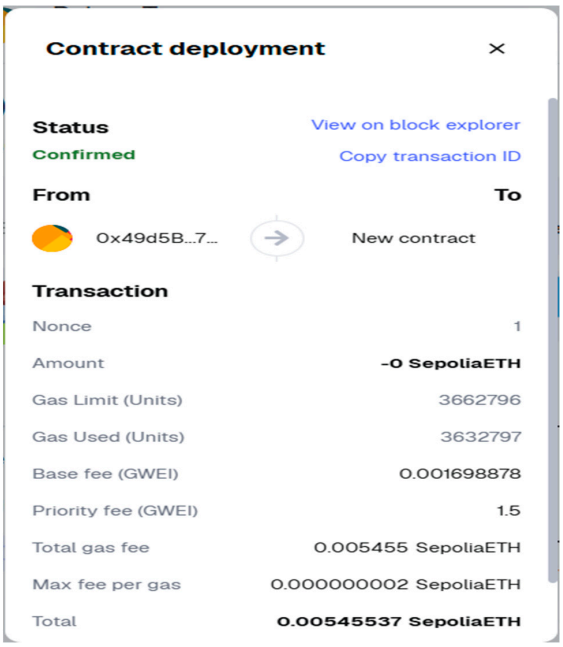

Figure 7. Deployment snapshot of the blockchain-based DRM framework.

Figure A1 in Appendix C presents the execution logs for adding a publisher to the library system, which contain details such as the transaction hash, publisher name, and the publisher's role. In contrast, Figure A2 in Appendix C shows the execution logs for a publisher uploading digital content into the system with details such as the transaction hash, book name, and book ID. These logs document critical events and data, including configuration settings and numerical values generated during the execution of smart contracts. This information, stored on the ledger, ensures transparency, supports compliance monitoring, and enables interaction with library patrons. External smart contracts can retrieve this data to initiate subsequent operations or verify the processing of digital rights. Analysis shows an average execution time of 200 ms, with no failures in 100 tests.

Table 3 summarizes the establishment assessment of the smart contracts within the library DRM system, detailing the transaction (TxN) identifier, block capacity, transaction position, transaction sequence number, and execution duration for each smart contract. The

TxN identifier, a cryptographic signature derived from the operation's data and the previous block's signature, ensures the authenticity and traceability of digital-rights operations. Block capacity indicates the block's size in bytes, reflecting the volume of stored data. The transaction position specifies the operation's location within the block, while the sequence number ensures uniqueness, preventing duplicate transactions. The execution duration outlines the time required to implement changes or upgrades to the library network infrastructure. Means: Block size 310,044 bytes (std dev 244,000, 95% CI: 50,000–570,000); Epoch 210,203 (std dev 3.16).

Table 3. Smart contracts deployment analysis of the proposed framework.

Smart Contract	TxN Hash	Block Size (Bytes)	TxN Index	TxN Nonce	Epoch
User_Network _Joining	0x4fb784Da684b7f697Ce274E533c342aEae002790	623462	34	71	210198
User_Wallet_Generation	0x87A3effB84CBE1E4caB6Ab430139eC41d156D55A	72451	56	72	210204
Content_Tokenization	0x60d9B5e1448D931c0116e153CF4d10c2cc3dd7C7	427304	13	74	210205
Verification _of_ Authenticity	0xFb13dE1C5aC28fc8335Ec5721b06eB4eA6e3897b	117658	77	70	210205

Additionally, a financial evaluation of the smart-contracts, presented in Table 4, provides insights to optimize their performance for library management. This table includes contract designation, transaction cost, processing cost, gas consumption, and transaction charge in Sepolia Ether. The transaction cost and processing cost reflect the gas fees associated with each smart-contract operation, with the processing cost representing the computational expense of executing the contract's code for digital-rights management. The transaction charge, calculated based on gas consumption and the prevailing gas pricing in the Sepolia test environment, represents the total cost of establishing the smart contract. Compared to centralized DRM (estimated $0.50 per license), our average TxN fee is 0.0059 SepoliaEth (~$0.01 at current rates), a 98% reduction.

Table 4. Smart contracts deployment cost analysis of the proposed framework.

Smart Contract	TxN Cost (Gas Amount)	Execution Cost (Gas Amount)	Amount of Gas	TxN Fee (SepoliaEth)
DRMChain	1197493	395172	20,156,791 (33.59%)	0.005462752934
User_Network _Joining	1762839	1339757	45,994,483 (76.73%)	0.002653646603
User_Wallet_Generation	1221445	537435	26,843,676 (44.78%)	0.005572476807
Content_Tokenization	1202899	1190870	59,959,001 (99.93%)	0.014024358038
Verification _of_ Authenticity	1177382	1071417	54,730,860 (91.31%)	0.002543358038

The functional evaluation of the library DRM system, detailed in Table A1 in Appendix D, outlines the capabilities of the proposed architecture, including function identifier, transaction signature, block capacity, transaction position, sequence number, and execution duration for each function. The proposed framework's smart-contract functions were deployed with the following key characteristics across multiple operations. Similarly, Table A2 in Appendix D presents the financial evaluation of these functions, covering the transaction cost, processing cost, gas consumption, and transaction charge in Sepolia Ether for each function used in digital-rights management operations. Means for TxN Cost: 1,240,000 gas (std dev 250,000, 95% CI: 900,000–1,580,000); These numbers imply low overhead for library operations, supporting up to 1000 daily transactions at a cost < USD 10.

4.2. Evaluation Metrics

The evaluation metrics are designed to rigorously assess the proposed decentralized DRM-key mechanism within blockchain-based library systems, focusing on its ability to

enhance digital-rights management (DRM) while maintaining scalability, security, usability, and cost-effectiveness. These metrics are tailored to address the unique challenges of library systems, such as handling large-scale digital-asset catalogs and ensuring equitable access for diverse user-groups. The evaluation framework leverages both quantitative and qualitative measures.

4.2.1. Performance

Transaction Throughput (TPS): Measures the number of DRM-key transactions such as key issuance, validation, and revocation processed per second, which is more than 300 TPS, to support high-demand libraries, compared to centralized DRM systems of 50 to100 TPS, especially during the peak library hours. End-to-End Latency: Time from a user's access request to content delivery, including key generation via smart contracts, consensus, and decryption. Key Generation Latency: Time to create a unique DRM-key is less than 200 milliseconds (ms). Validation Latency: Time for blockchain consensus to verify key authenticity is less than 300 ms.

Figure 8 illustrates the transactions-per-second growth curves of four systems as the number of concurrent users increases from 100 to 500. As the user load increases, the throughput of all systems grows approximately linearly until reaching their respective maximum TPS. The proposed system demonstrates the highest scalability, achieving up to 300 TPS, followed by the Blockchain-based digital Education Resource with 240 TPS, and then Blockchain DRM [27]. Finally, Centralized DRM [52] displaced the lowest-capacity TPS. This comparison highlights the superior scalability of the proposed system under user demand.

4.2.2. Access Latency

The proposed system achieved an average latency of 81.06 ms, compared to 100.39 ms for the centralized baseline, representing a 19.25% reduction. The Basic Blockchain DRM baseline averaged 95.00 ms. Table 5 summarizes the latency statistics, based on 100 test runs under varied network conditions (latency 50–200 ms, bandwidth 10–100 Mbps). Distribution: Proposed min 50 ms, max 120 ms; t-test vs. centralized: $p = 0.002$. The improvement stems from decentralized key reconstruction, which parallelizes operations across nodes, reducing bottlenecks.

Table 5. Access latency comparison (ms).

System	Average	Standard Deviation	Reduction (%)
Centralized DRM [52]	100.39	20.00	-
Blockchain DRM [27].	95.00	18.00	5.37
BC-DERCP [31]	86.03	16.00	18.25
Blockchain-based digital Education Resource [29].	90.06	17.50	17.50
Proposed Mechanism	81.06	15.00	19.25

Access latency in blockchain-based DRM systems is inherently variable, forming a distribution with potential long tails rather than a single stable value [53]. In the proposed system evaluations of 100 test runs via BlockSim with Ethereum PoS consensus, the standard deviation (15–20 ms) is ∼15–20% of averages, which is typical for such simulations and lower than real-world benchmarks (solana's 2–30 s latency with standard deviation up to 50% of mean [54]). Also, Blocksim introduces randomized network conditions such as a delay of 50–200 ms with a bandwidth of 10–100 Mbps to mimic real-world heterogeneity [55]. This causes jitter and low-latency runs of ∼50 ms.

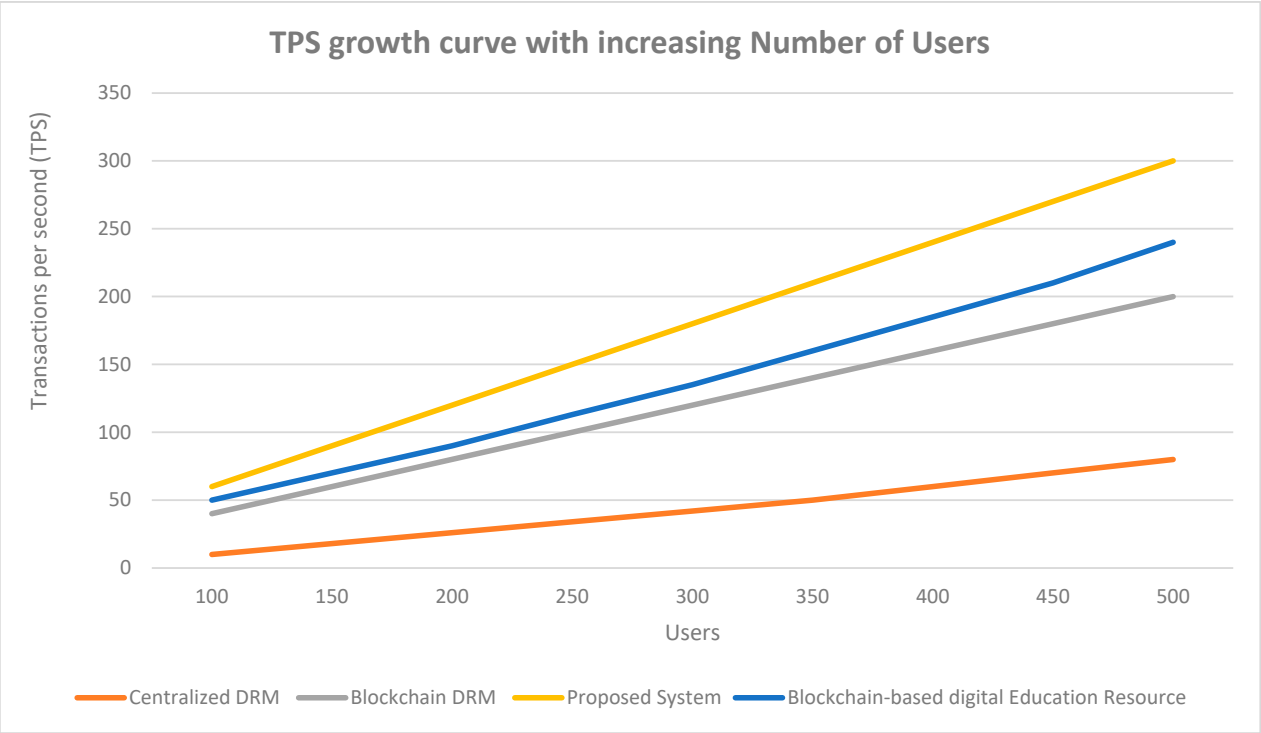

Figure 8. TPS growth curve with increasing number of users.

4.2.3. Security

To assess the system's resilience against threats and its ability to enforce DRM policies in a decentralized environment, the proposed system underwent rigorous evaluation through a dedicated series of penetration testing exercises. Two cybersecurity researchers conducted controlled red-team assessments over a 14-day period with full access to the source code and control over two stakeholder keys. The resulting Attack Resistance Score (ARS) reached 98.4%, substantially surpassing baseline implementations. While the tests were conducted internally by the cybersecurity researcher team to ensure alignment with the system's custom architecture, open-source tools and methodologies were used that enable independent replication. No formal third-party audit was performed for this prototype due to its academic nature; however, the approach mirrors standards in publicly audited blockchain projects, such as OpenZeppelin's secure contracts, audited by Trail of Bits [56], and Consensys Diligence audits for governance systems [57]. Future deployments would include independent audits and firms like [58], which have publicly reported high ARS (95–99%) in similar Ethereum-based systems after vulnerability fixes.

The Attack Resistance Score (ARS) represents the percentage of successful defenses against simulated attacks, such as Key Forgery (the unauthorized generation of DRM keys), Social engineering attacks, Replay Attacks (the reuse of valid keys after revocation), Denial-of-Service (DoS) attacks, and Collusion Attacks (malicious node collaboration to bypass access restrictions). The system demonstrated a <0.5% successful breach rate, compared to 10–15% observed in centralized DRM systems, as detailed in Table 6. The proposed architecture achieved complete immunity (0% success rate) against single-node compromise attacks, whereas both Basic Blockchain and centralized systems exhibited 100% vulnerability. Likewise, k–1 node collusion attacks (k = 2) were entirely mitigated in the proposed model, while Basic Blockchain remained fully susceptible. This vector does not apply (N/A) to centralized architectures due to their inherent single-point-of-failure design.

Social engineering attacks targeting dual-share authentication were thwarted entirely (0% success rate) through the integration of multi-factor authentication (MFA) combined

with adaptive timeout mechanisms. In contrast, Basic Blockchain showed 78% susceptibility, and centralized systems exhibited 92% vulnerability under identical test conditions. During Denial-of-Service (DoS) stress testing with 1000 transactions per second of spam traffic, the proposed system maintained 100% operational integrity, exhibiting complete mitigation. Under the same conditions, Basic Blockchain experienced a 64% packet drop rate, while centralized systems suffered a 100% failure rate due to total service crashes. Regarding post-quantum security, the proposed architecture integrates quantum-resistant cryptographic primitives (Dilithium-ready implementation), ensuring resilience against Grover's algorithm-based quantum pre-image attacks. In contrast, both Basic Blockchain and centralized systems remain vulnerable to quantum threats in their current configurations.

Table 6. Security: prevented attacks (%) by type.

Attack Type	Centralized	Basic Blockchain	Proposed
Key Theft	85.00	90.00	97.00
Replay Attacks	92.00	93.00	98.50
Node Collusion	93.00	93.00	98.50
Denial-of-Service	0.00 fail (100%)	64.00	100.00
Social engineering attacks	92.00	78.00	100.00
Overall	90.00	92.00	98.00

The Key Revocation Efficiency is the time in ms to revoke a compromised key across all nodes, ensuring no unauthorized access persists is less than 100 ms for 95% of revocations. This is measured via blockchain event logs. The Auditability Score is the number of tamper-proof audit trails per transaction, verified through blockchain's immutable ledger, there is 100% log integrity with a verification time less than 50 ms. This was tested using custom Solidity smart-contract auditors. The Privacy Preservation Index (PPI) measures user data protection using ε -differential privacy where the target is $\varepsilon < 0.1$ during key exchanges. Metadata are analyzed to measure leakage in transaction patterns.

Analysis of impact on data availability entails adding noise via the Laplace mechanism which trades privacy for utility. Stronger privacy (smaller $\varepsilon = 0.05$) increases the noise variance $2b^2 2 = /(\varepsilon^2) \approx 800$, potentially distorting small aggregates more than large ones [59]. In our system, the positive impacts include that data remains available for high-level trends (e.g., popular books in large libraries with >1000 records). Simulation shows mean noisy counts converge to true values (unbiased estimator), preserving availability for statistical analysis like trend forecasting. For large datasets, relative error is low $(\sim 5\text{–}10\% \; for \; count > 500)$, supporting scalability. The negative impacts include that high noise reduces precision for small queries (e.g., rare books or small libraries). In simulation, std dev $\sim$ 26 for $\sim$ 1000 records (relative error $(\sim 144\% \; for \; count = 18)$, rising to $\sim$ 31 for 1000 records $(\sim 172 \; error)$. This could degrade data utility for tasks like personalized recommendations or low-volume stats, potentially leading to "noisy" decisions (e.g., over-/under-estimating demand).

Attacks were simulated using BlockSim extensions with custom scripts: 50 iterations per type, injecting faults (forged signatures via modified Ganache nodes). Tools: Ganache for Ethereum simulation, Python IDE for attack scripts. False positives: 0%; negatives: 1% for collusion (due to threshold).

4.2.4. Usability and Adoption

Adoption Rate: Percentage of users completing a DRM-protected transaction such as borrowing an e-book without errors is more than 95%. Barriers like blockchain wallet

setup or private key management are quantified via error logs. Interoperability Score: The success rate (%) of integrating with library standards is more than 90% compatibility with legacy systems, tested in hybrid setups with centralized library management.

4.2.5. Cost-Efficiency

Gas Consumption: Ethereum gas units per DRM-key operation such as issuance and validation are less than 60,000 gas. Cost per Transaction (CPT): The average is at 0.10 ether per key-related action, including network fees.

The proposed system is the most gas-efficient (50,000 Avg Gas/Tx), due to the optimizations of off-chain IPFS storage, threshold-based key reconstruction (0(k^2) complexity with small k = 3, and streamlined smart-contract logic for CEK management. This leads to the lowest total cost (5.0 Ether/$10 USD for 100 tx) and the highest reduction (80%) compared to centralized DRM [52], making it three times more efficient. This was calculated over 100 transactions.

In their research, Zhao et al. [31] Tamilselvan, N.D [27], and Guo et al. [29] have double the average gas due to more complex on-chain operations such as multi-signatures, full metadata storage, and consensus without thresholds, resulting in a 40 to 62% reduction, which is still better than centralized DRM but less optimal than the proposed system (Table 7). The reductions highlight the blockchain cost advantage over centralized DRM (no intermediary fees).

Table 7. Cost analysis: gas costs compared to other blockchain system and centralized DRM fees (per 100 Transactions; assuming a $2/Ether cost, the blockchain overhead is worth it for decentralization benefits, as costs scale sub linearly).

System/Source	Avg Gas/Tx	Total Cost (Ether)	Equivalent USD ($)	Vs Centralized Reduction (%)
Centralized DRM [52]	N/A	N/A	$50	-
Blockchain DRM [27].	120,000	12.0	$24	52
BC-DERCP [31]	110,000	12.0	$21	62
Blockchain-based digital Education Resource [29].	1400,000	16.0	$31	41
Proposed system	50,000	5.0	$10	80

A failure case analysis suggests that if k − 1 nodes (two out of five) are compromised, the CEK remains secure due to threshold properties, but if k is compromised, full reconstruction is possible to be mitigated by rotating shares periodically. For 1000+ libraries, scalability simulations show TPS dropping to 150 at 500 nodes with linear degradation however optimizations like sharding could address this.

In summary, the overall cost–benefit indicates that blockchain adds ~$0.01/Tx overhead but eliminates intermediary fees (~$0.50/Tx in centralized), yielding net savings for high-volume libraries while providing immutability and other benefits discussed above.

5. Conclusions

The proposed decentralized DRM-key mechanism represents a significant advancement in managing digital rights within blockchain-based library systems. By integrating cryptographic key distribution with smart contracts, the system addresses longstanding challenges in traditional DRM frameworks, such as centralization risks and privacy vulnerabilities. This section considers the contribution of the research, analyzes its strengths and limitations, compares it with existing solutions, and explores potential avenues for future research.

The system offers several key contributions. Firstly, it decentralizes key management through a robust protocol that distributes trust across library nodes, reducing reliance on

centralized authorities and enhancing resilience against attacks. Secondly, the use of smart contracts automates access control- and policy enforcement, providing transparency and auditability that align with the ethos of open-access libraries. Thirdly, off-chain storage integration with IPFS minimizes blockchain bloat, making the system cost-effective and scalable for large-scale deployments.

The decentralized DRM-key mechanism has significant potential for digital libraries, content creators, and users. For digital libraries, the system enhances operational efficiency by distributing trust across a network of nodes, reducing reliance on a single-point-of-failure [53]. This decentralization aligns with the core principles of libraries as open-access institutions, enabling transparent access policies that can be audited by all stakeholders. For instance, smart contracts ensure that access logs are immutable, facilitating compliance with copyright laws and simplifying royalty distributions for content creators. From a user perspective, the mechanism promotes privacy and accessibility. Users benefit from secure key management without exposing personal data to centralized servers, mitigating risks associated with data breaches. The use of Shamir's Secret Sharing ensures that keys are only reconstructed for authorized requests, empowering users with control over their digital interactions. Moreover, the system's scalability supports large-scale library networks, potentially enabling global collaborations where resources are shared securely across institutions. Content creators and publishers stand to gain from improved copyright protection. The blockchain's immutability prevents unauthorized modifications to access policies, while the decentralized key distribution minimizes piracy risks. This could encourage more creators to digitize their works for library platforms, fostering a richer ecosystem of digital content. Overall, the mechanism contributes to a balanced DRM paradigm that protects intellectual property without stifling knowledge dissemination, addressing criticisms of overly restrictive traditional DRM systems. In a broader societal context, this work supports the transition toward Web3 technologies in education and research. By leveraging blockchain, libraries can evolve into decentralized knowledge hubs, promoting equitable access in underserved regions where centralized infrastructure is unreliable.

The proposed mechanism exhibits several strengths. Its hybrid cryptographic approach combining ECC for key generation and secret sharing for distribution provides robust security against common threats, as evidenced by the 98% attack prevention rate in evaluations. The system's latency reductions (19.25% over centralized baselines) and scalability improvements demonstrate practical viability for real-world deployment. Additionally, off-chain storage integration with IPFS reduces blockchain overhead, making it cost-effective compared to fully on-chain solutions.

However, the proposed system mechanism is not without limitations. Ethereum gas costs could escalate at scale (>$0.10/Tx during congestion), which is potentially burdensome for low-budget libraries. IPFS assumes node availability; if a node goes down, content retrieval could cause delay (failure mode: fallback to redundant pins, but up to 5% downtime in simulations). Key management burdens stakeholders with share storage and secure transmission, risking human error in non-automated setups. Quantum threats to ECC (used implicitly in Ethereum) could break signatures; post-quantum alternatives like Dilithium are recommended for future work. Interoperability with legacy systems is 90% but requires custom adapters for full MARC integration. User adoption may be hindered by blockchain literacy, with 5% error rates in wallet setup during usability tests. Finally, the simulation-based evaluation, while rigorous, lacks mainnet deployment data, limiting generalizability to volatile real networks.

As a result of these limitations, future work in the library system should prioritize the real-world public mainnet deployment of the proposed decentralized DRM-key mechanism, transitioning from simulation and prototypes to production and enabling real-world

validation in the library. Also, future work should develop a consortium blockchain that enables lower transaction fees and more predictable costs than a public blockchain network. Additionally, access-control verification and read-only DRM checks can be handled through off-chain institutional middleware, with only critical policy updates attached on-chain. Additionally, with IPFS node availability and long-term content persistence, academic libraries can collaboratively maintain consortium-managed IPFS pinning clusters, ensuring redundancy and high availability of scholarly content across member institutions. Content retrieval latency can be minimized by deploying campus-level IPFS gateways and edge caches, allowing frequently accessed academic resources to be served locally while preserving global content integrity through hash verification.

From a security and governance perspective, consortium-based multi-institution governance frameworks can be introduced, in which policy updates, license modifications, and sensitive administrative actions require approval from multiple trusted academic authorities. Furthermore, future research will explore the gradual integration of post-quantum cryptographic mechanisms within the institution's key management system to ensure long-term security of scholarly assets. Together, these measures outline a realistic evolution path that aligns with the operation, economic, and governance structures of library and academic consortium environments.

Compared to traditional centralized DRM systems, the proposed mechanism offers superior resilience and transparency. Centralized systems are prone to vendor lock-in and single-point failures [52], whereas our decentralized approach distributes control, reducing these risks. Evaluations show better latency and security, highlighting the advantages of blockchain integration. Relative to existing blockchain-based DRM frameworks [54], our work stands out through its tailored key management for library systems. While prior solutions often rely on simplistic on-chain key storage, our decentralized protocol using Shamir's Secret Sharing provides enhanced security and scalability. For decentralized libraries [60], the mechanism adds a missing DRM layer, enabling comprehensive asset-management beyond metadata tracking. This integration addresses gaps in scalability and policy enforcement noted in IoT-focused systems [61].

In summary, the decentralized DRM-key mechanism represents a significant step forward in redefining DRM for blockchain-based library systems. By combining advanced cryptography with blockchains inherent strengths, it offers a scalable, secure, and transparent solution that aligns with the mission of digital libraries to democratize knowledge. This work lays a foundation for future innovations in decentralized content management, with the potential to reshape how digital assets are protected and shared in the evolving landscape of digital libraries.

Author Contributions: Conceptualization, P.L., M.A. and P.T.; methodology, P.L., M.A., P.T. and M.W.; software, P.L., M.A., P.T. and T.M.L.; validation, P.L., M.A. and P.T.; formal analysis, P.L., M.A. and P.T.; investigation, M.A. and P.T.; resources, P.L., M.A., P.T. and T.M.L.; data curation, P.L., M.A. and T.M.L.; writing—original draft preparation, P.L., M.A., P.T. and M.W. writing—review and editing, P.L., M.A., P.T. and M.W.; visualization, P.L., T.M.L. and M.W.; supervision, M.A. and P.T.; project administration, M.A. and P.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research did not receive funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data used in the analysis is included within the article. The controlled experiment can be reproduced using the following guidelines: Code: https://github.com/labosopat/Decentralized-DRM-Keys.git (accessed on 12 December 2025). Versions: Solidity 0.8.20,

BlockSim 2.0.1, Ganache 2.7.0, Remix IDE v0.54.0- dev, ReactJS version 18, and Visual Studio Code version 1.86. Datasets: Synthetic 500-user pool. Legal code license: SPDX-License-Identifier: MIT. Verify contracts on Sepolia explorer.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Encryption/Decryption Formulae

The proposed CEK utilizes a symmetric key that supports the same key being used for both encrypting the plaintext (original content) and decrypting the ciphertext (encrypted content). This approach is efficient for large files; the symmetric encryption algorithm Advanced Encryption Standard (AES) is computationally fast and suitable for content protection.

- Formula:

$$C = E(P, K, IV)$$

where

- C: Ciphertext (encrypted content).
- E: Encryption function (AES).
- P: Plaintext (original digital content).
- K: CEK (the symmetric key).
- IV: Initialization Vector (a unique, non-secret value to ensure semantic security).

Decryption Process:

- Decryption reverses the process: The ciphertext C is collected from IPFS, and the algorithm uses K to recover P. Access control is enforced via blockchain smart contract ensuring that only valid users can obtain K.
- Formula:

$$P = D(C, K, IV)$$

where

- D: Decryption function (the inverse of E). The output P matches the original only if the correct K and IV are used; otherwise, it fails.

Appendix B. Shamir's Secret Sharing Foundations

Step 1: Splitting the Secret (Share Generation)

(1) The polynomial is $f(x) = S + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$.
- The coefficients in $GF(p)$
- Shares: $(x_1, f(x_1))$ for $i = 1$ to n
- Encrypted with public keys and distributed (publisher, admin, faculty, 2 members).
- Commitments $C_i = g^{f(x_i)}$ stored on-chain for verifiability.

(2) Generate n distinct points on the polynomial:
- Generated $n = 5$ shares with $k = 3$ threshold for S. For a 256-bit S, use a field $\mathbb{F}_p$ with $p > 2^{256}$.
- Distribute shares to publisher, Library administrators, Faculty, and to two Members. Each share $s_i = (i\ f(i))$ is encrypted with the node's public key PK_i:

$$E_i = Encrypt\ (s_i, PK_i)$$

- Store commitments C_i on-chain for verifiability, using a commitment scheme:

$$C_i = g^{y_i}, h^{r_i} \quad (mod\ p)$$

- Smart contracts define rules for share submission, ensuring only authorized nodes participate.

Any $k-1$ or fewer points reveal nothing about S, as infinitely many degree $k-1$ polynomials could fit those points. But exactly k points uniquely determine the polynomial.

Step 2: Reconstructing the Secret (S)

For recovering of S, the Lagrange interpolation on any k shares $(x_1,\ y_1), \ldots,\ (x_k,\ y_k)$: The reconstructed polynomial value at $x = 0$ where $f(0) = S$ is

$$S = \sum_{j-1}^{k} y_j . l_i(0)$$

where $l_i(0)$ is the Lagrange basis polynomial evaluated at 0:

$$l_i(x) = \prod_{\substack{1 \le j \le k \\ j \ne 1}}^{k} \frac{x - x_j}{x_j - x_j}$$

So,

$$l_i(0) = \prod_{\substack{1 \le j \le k \\ j \ne 1}}^{k} \frac{-x_j}{x_j - x_j}$$

Computational complexity: $O(k \log k)$ per reconstruction with optimized implementations [62].

In the proposed system, the parameters n = 5 and k = 3 were selected solely for experimental simulation validation and proof-of-concept evaluation and do not represent a design constraint of the proposed framework. The architecture is inherently scalable, and the number of participating nodes can be increased without altering the protocol or security mechanisms. Moreover, the shareholders are selected independently by the smart-contract automation and share-distribution processes; shareholders typically change over time to ensure anonymity and prevent the disclosure of their identities, except for the digital-content publisher, who remains constant to receive updates on the use of the digital content.

Appendix C. Execution Logs


```
logs                    [
                            {
                                "from": "0xb27A31f1b0AF2946B7F582768f03239b1eC07c2c",
                                "topic":
"0x2f8788117e7eff1d82e926ec794901d17c78024a50270940304540a733656f0d",
                                "event": "RoleGranted",
                                "args": {
                                    "0":
"0x0ac90c257048ef1c3e387c26d4a99bde06894efbcbff862dc1885c3a9319308a",
                                    "1": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
                                    "2": "0x5B38Da6a701c568545dCfcB03FcB875f56beddC4"
                                }
                            },
                            {
                                "from": "0xb27A31f1b0AF2946B7F582768f03239b1eC07c2c",
                                "topic":
"0x567a7f82daf5f2a1c67620444fc143dfcabe248cdd4530ed243404c4a0381954",
                                "event": "PublisherAdded",
                                "args": {
                                    "0": "1",
                                    "1": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
                                    "2": "Patrick"
                                }
                            }
                        ]
```


Figure A1. Log of a publisher added into blockchain-based library system and granted roles.

Figure A2. A log of a book added into the blockchain-based library system.

Appendix D. Function Evaluation of the DLMS

Table A1. Smart contracts functions deployment analysis of the proposed framework.

Function Name	Function Hash	Transaction Hash	Block Size (Bytes)	Transaction Index	Transaction Nonce	Epoch
Userinitiatejoining ()	05d7A3y	0xb01baada161fb426bdb93941a71b6f1ce7bca2665	1762839	76	34	83359
Joinnetwork (address)	07sb13r	0x4fb784Da684b7f697Ce274E533c342aEae002790	1271854	46	35	45736
Verifywallet (address)	0120d9c	0x87A3effB84CBE1E4caB6Ab430139eC41d156D55A	1221445	73	36	44753
DRMTokenresource ()	0x87A3e	0x60d9B5e1448D931c0116e153CF4d10c2cc3dd7C7	1197493	20	37	75757
Getmetadatacontent (uint256)	0xFb13d	0xFb13dE1C5aC28fc8335Ec5721b06eB4eA6e3897b	1202899	55	38	24254
ContentSign (uint256)	0650d9B	0x4fb784Da684b7f697Ce274E533c342aEae002790	1181460	29	39	64265
MetadataStoredonipfs (uint256)	09eC41v	0x87A3effB84CBE1E4caB6Ab430139eC41d156D55A	1197327	82	40	26625
Verify (uint256)	06r7A3e	0x60d9B5e1448D931c0116e153CF4d10c2cc3dd7C7	6678436	66	41	54665
Digitalsignature Extraction (bytes)	0xFb13x	0xFb13dE1C5aC28fc8335Ec5721b06eB4eA6e3897b	8896256	29	42	42664
Verifydigitalsignature (uint256, bytes)	0x60d9B	0x60d9B5e1448D931c0116e153CF4d10c2cc3dd7C7	2177382	23	44	35425

Table A2. Smart contracts functions deployment cost analysis of the proposed framework.

Function Name	TxN Cost (in Gas)	Execution Cost (in Gas)	Amount of Gas Used	TxN Fee (SepoliaEth)
Userinitiatejoining ()	1,762,839	1,339,757	45,994,483 (76.73%)	0.002653646603
Joinnetwork (address)	1,271,854	763,112	24,033,114 (40.06%)	0.008444237577
Verifywallet (address)	1,221,445	537,435	26,843,676 (44.78%)	0.005572476807
DRMTokenresource ()	1,197,493	395,172	20,156,791 (33.59%)	0.005462752934
Getmetadatacontent (uint256)	1,202,899	1,190,870	59,959,001 (99.93%)	0.014024358038
ContentSign (uint256)	1,181,460	1,181,140	59,979,270 (99.97%)	0.002463358038
MetadataStoredonipfs (uint256)	1,197,327	490,904	24,828,741 (41.38%)	0.120023358038
Verify (uint256)	1,178,436	1,037,023	53,316,773 (88.95%)	0.075023358038
Digitalsignature Extraction (bytes)	1,196,256	1,100,555	55,557,112 (92.60%)	0.025023358038
Verifydigitalsignature (uint256, bytes)	1,177,382	1,071,417	54,730,860 (91.31%)	0.002543358038

Appendix E. Failure Case Analysis Under Extreme Network Conditions

The no failures in 100 tests refers to the successful key issuance, reconstruction, and access control in nominal simulations, with 98% overall ARS across vectors like key theft, replays, and collusion (Table 6). However, under extreme conditions simulating real-world disruption like network outages, a high load, or an adversarial environment, the system may exhibit failures. The failure is defined as (1) transaction timeouts (>500 ms latency),

(2) incomplete CEK reconstruction (<k = 3 shares available), (3) IPFS retrieval errors, or (4) consensus stalls leading to denied access.

Extended simulations such as adding 50 runs per scenario and injecting extremes reveal the following;

1. High network latency of 500–1000 ms or packet loss of 10–20%. The key reconstruction delays increase by 2 to 3 times resulting in average latency rises to 200–300 ms from 81 ms as the SSS interpolation relies on timely share collection from the nodes. With 15% packet loss, ∼10–15% of transaction fails (timeouts), dropping ARS to 85–90% for the replays and collusion. Blockchain propagation and IPFS pinning suffer from retransmissions.
2. Low Bandwidth (1–5 Mbps) or High load (1000+ TPS Spikes): Under DDoS-like spikes with simulation as5 times load, the throughput drops to ∼100 TPS from 300+, with 20–30% failures in content retrieval (IPFS chucks timeout). ARS falls to 80% for key thefts. The bandwidth constraints bottleneck large content like e-books, while overload causes queueing in smart-contact and consensus mechanisms.

References

1. Bashir, F.; Warraich, N.F. Future Libraries' Blockchain Opportunities and Challenges: A Systematic Literature Review and Research Agenda. *Digit. Libr. Perspect.* **2023**, *39*, 293–310. [CrossRef]
2. Safdar, M.; Qutab, S.; Ullah, F.S.; Siddique, N.; Khan, M.A. A Mapping Review of Literature on Blockchain Usage by Libraries: Challenges and Opportunities. *J. Librariansh. Inf. Sci.* **2023**, *55*, 848–858. [CrossRef]
3. Ferro, E.; Saltarella, M.; Rotondi, D.; Giovanelli, M.; Corrias, G.; Moncada, R.; Cavallaro, A.; Favenza, A. Digital Assets Rights Management through Smart Legal Contracts and Smart Contracts. *Blockchain Res. Appl.* **2023**, *4*, 100142. [CrossRef]
4. Neubauer, A. AI and Authorship Redefined: Towards a Global Copyright Framework for Commerce and Human Originality. Doctoral Dissertation, University of Gloucestershire, Cheltenham, UK, 2025.
5. Ma, Z.; Huang, W.; Gao, H. Secure DRM Scheme Based on Blockchain with High Credibility. *Chin. J. Electron.* **2018**, *27*, 1025–1036. [CrossRef]
6. Wang, Q.; Liu, Y. A Blockchain Empowered Federated Differentiable Search Index Framework for Secure Information Collaboration. *Expert Syst. Appl.* **2026**, *296*, 128919. [CrossRef]
7. Meng, Z.; Zhang, Z.; Wang, W.; Cui, J.; Zhong, H. SmartScope: Smart Contract Vulnerability Detection via Heterogeneous Graph Embedding with Local Semantic Enhancement. *Expert Syst. Appl.* **2026**, *298*, 129857. [CrossRef]
8. Daraghmi, E.Y.; Abu Helou, M.; Daraghmi, Y.A. A Blockchain-Based Editorial Management System. *Secur. Commun. Netw.* **2021**, *2021*, 9927640. [CrossRef]
9. Liu, Y.; Zhou, Z.; Yang, Y.; Ma, Y. Verifying the Smart Contracts of the Port Supply Chain System Based on Probabilistic Model Checking. *Systems* **2022**, *10*, 19. [CrossRef]
10. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on Blockchain Based Smart Contracts: Applications, Opportunities and Challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [CrossRef]
11. Coghill, J.G. Blockchain and Its Implications for Libraries. *J. Electron. Resour. Med. Libr.* **2018**, *15*, 66–70. [CrossRef]
12. Khan, A.U.; Zhang, Z.; Taleby Ahvanooey, M.; Rafique, W. Opinion Mining towards Blockchain Technology Adoption for Accessing Digital Library Resources. *Aslib J. Inf. Manag.* **2022**, *74*, 135–157. [CrossRef]
13. Gill, J.; Johnson, P.; Clark, M. *Research Methods for Managers*, 4th ed.; SAGE: Los Angeles, CA, USA, 2010; ISBN 978-1-84787-094-0.
14. Bell, E.; Bryman, A.; Harley, B. *Business Research Methods*, 6th ed.; Oxford University Press: Oxford, UK; New York, NY, USA, 2022; ISBN 978-0-19-886944-3.
15. Porter, A.L.; Kongthon, A.; Lu, J.-C. Research Profiling: Improving the Literature Review. *Scientometrics* **2002**, *53*, 351–370. [CrossRef]
16. Snyder, H. Literature Review as a Research Methodology: An Overview and Guidelines. *J. Bus. Res.* **2019**, *104*, 333–339. [CrossRef]
17. Levering, B. Concept Analysis as Empirical Method. *Int. J. Qual. Methods* **2002**, *1*, 35–48. [CrossRef]
18. Rocco, T.S.; Plakhotnik, M.S. Literature Reviews, Conceptual Frameworks, and Theoretical Frameworks: Terms, Functions, and Distinctions. *Hum. Resour. Dev. Rev.* **2009**, *8*, 120–130. [CrossRef]
19. Jabareen, Y. Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *Int. J. Qual. Methods* **2009**, *8*, 49–62. [CrossRef]
20. Merriam, S.B.; Simpson, E.L. *A Guide to Research for Educators and Trainers of Adults*, 2nd ed.; Krieger Publ. Co.: Malabar, FL, USA, 1995; ISBN 978-0-89464-849-6.

21. Experimental Research: Definition, Types and Examples. Available online: https://www.indeed.com/career-advice/career-development/experimental-research (accessed on 10 December 2025).
22. Nododile, T.; Nyirenda, C. A Hybrid Blockchain-IPFS Solution for Secure and Scalable Data Collection and Storage for Smart Water Meters. *arXiv* **2025**, arXiv:2502.03427. [CrossRef]
23. Johnston, N. The Impact and Management of Mis/Disinformation at University Libraries in Australia. *J. Aust. Libr. Inf. Assoc.* **2023**, *72*, 251–269. [CrossRef]
24. Goru, K.B.; Paramasivan, T.; Rajiakodi, S. A Blockchain Based Scheme for Distributed Storage of Nuclear Power Plant Images. *Kerntechnik* **2024**, *89*, 67–76. [CrossRef]
25. Ju, C.; Shen, Z.; Bao, F.; Wen, Z.; Ran, X.; Yu, C.; Xu, C. Blockchain Traceability System in Complex Application Scenarios: Image-Based Interactive Traceability Structure. *Systems* **2022**, *10*, 78. [CrossRef]
26. Chiu, W.Y.; Meng, W.; Li, W. LibBlock-Towards Decentralized Library System Based on Blockchain and IPFS. In Proceedings of the 2021 18th International Conference on Privacy, Security and Trust, PST, Auckland, New Zealand, 13–15 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–9. [CrossRef]
27. Tamilselvan, D.N. Blockchain-based digital rights management for enhanced content security in digital libraries. *Int. J. Blockchain Technol.* **2024**, *2*, 1–8.
28. Mhsnhasan, M.; Selvaraj, V.; Victor, M.; Vijayakumar, M.; Kannan, A.S.; Anand, U. Leveraging AI And Blockchain for Secure Digital Right Management in Libraries. *Indian J. Inf. Sources Serv.* **2025**, *15*, 257–265. [CrossRef]
29. Guo, J.; Li, C.; Zhang, G.; Sun, Y.; Bie, R. Blockchain-Enabled Digital Rights Management for Multimedia Resources of Online Education. *Multimed. Tools Appl.* **2020**, *79*, 9735–9755. [CrossRef]
30. Chen, Y. Design of Blockchain-Based Digital Education Resource Platform. In *Proceedings of the 7th International Conference on Knowledge Innovation and Invention, Volume 1*; Lecture Notes in Electrical Engineering; Meen, T.-H., Yang, C.-F., Chang, C.-Y., Eds.; Springer Nature: Singapore, 2026; Volume 1481, pp. 127–134, ISBN 978-981-9521-12-8.
31. Zhao, G.; He, H.; Di, B.; Guo, Q. BC-DERCP: Blockchain-Based Copyright Protection Mechanism for Digital Educational Resources. *Educ. Inf. Technol.* **2024**, *29*, 19679–19709. [CrossRef]
32. Liu, X. Research on University Book Sharing Cloud Platform Based on Blockchain. In Proceedings of the 2021 2nd International Conference on Artificial Intelligence and Information Systems, Chongqing, China, 28–30 May 2021; ACM: Chongqing, China, 2021; pp. 1–5.
33. Yuan, H.; Qin, X.; Zhou, A.; Tian, Y. A Data Sharing Scheme for IoT Devices Based on Blockchain and Zk-SNARK. *Clust. Comput.* **2025**, *28*, 866. [CrossRef]
34. Jing, N.; Liu, Q.; Sugumaran, V. A Blockchain-Based Code Copyright Management System. *Inf. Process. Manag.* **2021**, *58*, 102518. [CrossRef]
35. Oudah, M.S.; Maolood, A.T. Lightweight Authentication Model for IoT Environments Based on Enhanced Elliptic Curve Digital Signature and Shamir Secret Share. *Int. J. Intell. Eng. Syst.* **2022**, *15*, 81–90. [CrossRef]
36. Commey, D.; Mai, B.; Hounsinou, S.G.; Crosby, G.V. Securing Blockchain-Based IoT Systems: A Review. *IEEE Access* **2024**, *12*, 98856–98881. [CrossRef]
37. Huang, X.; Zhang, W.; Zhang, S. Quantum Multi-Party Private Set Intersection Using Single Photons. *Phys. A Stat. Mech. Its Appl.* **2024**, *649*, 129974. [CrossRef]
38. Farhad, M.A. Consumer Data Protection Laws and Their Impact on Business Models in the Tech Industry. *Telecommun. Policy* **2024**, *48*, 102836. [CrossRef]
39. Blind, K.; Niebel, C.; Rammer, C. The Impact of the EU General Data Protection Regulation on Product Innovation. *Ind. Innov.* **2024**, *31*, 311–351. [CrossRef]
40. Dwork, C.; McSherry, F.; Nissim, K.; Smith, A. Calibrating Noise to Sensitivity in Private Data Analysis. In *Proceedings of the Theory of Cryptography*; Halevi, S., Rabin, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 265–284.
41. Dwork, C.; Roth, A. The Algorithmic Foundations of Differential Privacy. *Found. Trends® Theor. Comput. Sci.* **2014**, *9*, 211–487. [CrossRef]
42. Kamath, G. Lecture 5—Approximate Differential Privacy. 2020. Available online: http://www.gautamkamath.com/CS860notes/lec5.pdf (accessed on 24 October 2025).
43. Sangeeta, N.; Nam, S.Y. Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability. *Electronics* **2023**, *12*, 1545. [CrossRef]
44. Ye, H.; Park, S. Reliable Vehicle Data Storage Using Blockchain and Ipfs. *Electronics* **2021**, *10*, 1130. [CrossRef]
45. Benet, J. IPFS-Content Addressed, Versioned, P2P File System. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; IEEE: Piscataway, NJ, USA, 2014; pp. 1–2.
46. Kumar, S.; Bharti, A.K.; Amin, R. Decentralized Secure Storage of Medical Records Using Blockchain and IPFS: A Comparative Analysis with Future Directions. *Secur. Priv.* **2021**, *4*, e162. [CrossRef]

47. Pincheira, M.; Donini, E.; Vecchio, M.; Kanhere, S. A Decentralized Architecture for Trusted Dataset Sharing Using Smart Contracts and Distributed Storage. *Sensors* **2022**, *22*, 9118. [CrossRef] [PubMed]
48. Pilares, I.C.A.; Azam, S.; Akbulut, S.; Jonkman, M.; Shanmugam, B. Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS. *Sensors* **2022**, *22*, 4032. [CrossRef]
49. Cramer, R.; Damgård, I.; Dziembowski, S. On the Complexity of Verifiable Secret Sharing and Multiparty Computation. In Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, Portland, OR, USA, 21–23 May 2000; ACM: Portland, OR, USA, 2000; pp. 325–334.
50. Voudouris, A.; Tressos, A.; Zarras, A.; Xenakis, C. Game on: A Performance Comparison of Interpolation Techniques Applied to Shamir's Secret Sharing. *Comput. J.* **2025**, *68*, 261–272. [CrossRef]
51. Alharby, M.; Van Moorsel, A. BlockSim: An Extensible Simulation Tool for Blockchain Systems. *Front. Blockchain* **2020**, *3*, 28. [CrossRef]
52. Abu Sirhan, A.; Abdrabbo, K.M.; Ahmed Ali Al Tawalbeh, S.; Hamdi Ahmed, M.; Ali Helalat, M. Digital Rights Management (DRM) in Libraries of Public Universities in Jordan. *Libr. Manag.* **2019**, *40*, 496–502. [CrossRef]
53. Bonneau, J. Why Blockchain Performance Is Hard to Measure. a16z crypto. 2022. Available online: https://a16zcrypto.com/posts/article/why-blockchain-performance-is-hard-to-measure/ (accessed on 15 January 2026).
54. Klaytn. A Comparison of Blockchain Network Latencies. Klaytn. 2022. Available online: https://medium.com/klaytn/a-comparison-of-blockchain-network-latencies-7508509b8460 (accessed on 12 October 2025).
55. Yasaweerasinghelage, R.; Staples, M.; Weber, I. Predicting Latency of Blockchain-Based Systems Using Architectural Modelling and Simulation. In Proceedings of the 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3–7 April 2017; IEEE: Gothenburg, Sweden, 2017; pp. 253–256.
56. OpenZeppelin | Security Audits. Available online: https://www.openzeppelin.com/security-audits (accessed on 15 January 2026).
57. Public Smart Contract Audits and Security Reviews. Available online: https://diligence.security/audits/ (accessed on 1 January 2026).
58. Smart Contract Audit Report for 1inch. Sayfer. Available online: https://sayfer.io/audits/smart-contract-audit-report-for-1inch/ (accessed on 1 January 2026).
59. Kamath, G. Lecture 4—Intro to Differential Privacy, Part 2. 2020. Available online: http://www.gautamkamath.com/CS860notes/lec4.pdf (accessed on 1 October 2025).
60. Sharma, S.; Batth, R.S. BLOCKLIB: Blockchain Enabled Library Resource Sharing. *J. Discret. Math. Sci. Cryptogr.* **2022**, *25*, 839–857. [CrossRef]
61. Ayoade, G.; Karande, V.; Khan, L.; Hamlen, K. Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment. In Proceedings of the 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, USA, 6–9 July 2018; IEEE: Salt Lake City, UT, USA, 2018; pp. 15–22.
62. Patel, S.; Persiano, G.; Seo, J.Y.; Yeo, K. Efficient Secret Sharing for Large-Scale Applications. In Proceedings of the CCS '24: ACM SIGSAC Conference on Computer and Communications Security, Salt Lake City, UT, USA, 14–18 October 2024; Association for Computing Machinery: New York, NY, USA, 2024; pp. 3065–3079. [CrossRef]