ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov091

Decentralized Access Control Using Blockchain for Academic Publishing Repositories in Higher Institutions in Nigeria

Emmanuel Eturpa Salami[1]; Yunisa Sunday[2]; Caleb Lateef Umoru[3]; Attah Joshua[4]

[1]Department of Software Engineering, Confluence University of Science and technology, Osara Kogi State, Nigeria
[2]Department of Cybersecurity Science, Confluence University of Science and Technology, Osara Kogi State, Nigeria
[3]Department of Cybersecurity, Confluence University of Science and Technology, Osara, Kogi State Nigeria
[4]Department of Information Technology Confluence University of Science and technology, Osara Kogi State, Nigeria

Publication Date: 2025/11/13

Abstract: Academic publishing repositories in developing nations often face severe challenges in enforcing secure and transparent access control, exacerbated by centralized authority, weak audit trails, and data manipulation risks. This research proposes a decentralized access control system using Hyperledger Fabric blockchain and smart contracts to ensure secure, transparent, and tamper-proof data access in academic repositories. Using a constructive research methodology, the study develops and evaluates a blockchain-integrated framework tailored for repositories like DSpace. The methodology includes model-driven engineering, smart contract development in GoLang, PKI-based identity control, and simulation via Dockerized microservices. Empirical evaluation reveals superior performance: 250ms transaction latency, 70 TPS throughput, and complete prevention of unauthorized access attempts, outperforming centralized models. Security analysis and user surveys among repository stakeholders indicate enhanced transparency, trust, and system usability. The findings demonstrated that decentralized models significantly improve access control without compromising usability. The research contributes both theoretically and practically to secure scholarly communication in Nigeria. It aligns with evolving open access initiatives, builds local technical capacity, and proposes a replicable model for enhancing repository trustworthiness across universities in Nigeria. Future work can explore scalable, privacy-preserving extensions and AI-driven smart contract automation.

Keywords: *Blockchain, Access Control, Academic Repositories, Smart Contracts, Decentralization, Hyperledger, Open Access*.

How to Cite: Emmanuel Eturpa Salami; Yunisa Sunday; Caleb Lateef Umoru; Attah Joshua (2025) Decentralized Access Control Using Blockchain for Academic Publishing Repositories in Higher Institutions in Nigeria. *International Journal of Innovative Science and Research Technology*, 10(11), 343-351 https://doi.org/10.38124/ijisrt/25nov091

I. INTRODUCTION

In higher institutions across Nigeria, academic publishing repositories play a pivotal role in preserving, disseminating, and promoting access to scholarly outputs. The proliferation of digital repositories has revolutionized academic publishing by enhancing visibility and accessibility of scholarly outputs. However, the security and control of these platforms especially in developing nations are predominantly centralized, leading to vulnerabilities such as unauthorized access, plagiarism, identity theft, and data tampering (Abeywardena et al., 2023). Inadequate infrastructure, lack of audit mechanisms, and weak regulatory oversight further aggravate these issues (Okon & Eze, 2022). Also, the growing reliance on repositories such as DSpace and institutional digital archives, critical security and transparency gaps remain prevalent. Many repositories operate under centralized access control models, which frequently suffer from weak auditability, susceptibility to unauthorized modifications, and administrative override of author permissions (Njoku et al., 2023). Blockchain technology, with its decentralized ledger, tamper-resistant design, and smart contract capabilities, has emerged as a promising solution to such challenges. Permissioned blockchain systems like Hyperledger Fabric enable fine-grained, immutable governance of access permissions in a distributed environment, thereby reducing reliance on a single administrative authority (Novotny et al., 2018). Nigerian research institutions have begun to explore blockchain applications for authenticating academic

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov091

credentials and securing personal records (Akuma et al., 2024), while studies on transcript verification and certificate issuance report strong potential for tamper-proof validation using blockchain frameworks. These pilot initiatives affirm the relevance of decentralized ledger systems in the context of higher education in Nigeria. Blockchain technology presents a transformative opportunity to redesign access control in a decentralized, tamper-evident, and transparent manner. Despite significant progress in applying blockchain in health, finance, and logistics, its application in academic repository security, particularly in under-resourced nations, remains underexplored. It specific application for access control in academic repositories has gained very little attention. Also, there is no published study that integrates blockchain-enabled smart contracts for securing DSpace-style repository access in Nigerian universities.

- *Traditional Access Control in Academic Repositories*

Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are common models for regulating repository access (Zhang et al., 2022). However, their centralized management makes them susceptible to single points of failure. According to (Idris et al, 2021) most academic institutions in developing nations lack infrastructure to enforce and audit digital rights management. They also observed that existing systems rarely ensure author-controlled permissions and audit trails, which leads to weak trust and poor institutional repository adoption. Although Blockchain technologies, including Ethereum and Hyperledger, have shown promise in enforcing distributed, cryptographically enforced policies via smart contracts (Liang et al., 2021) observed that integration into academic workflows remains a nascent area. According to Fasola et al, (2024) there is an institutional readiness and blockchain adoption awareness among librarians which is steadily rising, but barriers such as technophobia, limited infrastructure, and lack of technical competence has slowed down the adoption rate. Their findings underscore both the feasibility and the challenge of deploying decentralized systems for scholarly publishing in Nigeria. However, there are Opportunities to leverage blockchain as tool to improve transparency in peer review, empower authors to define access policies, and ensure immutable logs of all repository interactions. Given the strategic importance of open access and scholarly visibility for African research highlighted by initiatives like LIBSENSE and the National Repository of Nigeria (Mdpi blog, 2025) a blockchain-enabled access control mechanism could significantly advance institutional repository integrity, empower researchers, and promote trust in digital scholarly infrastructure.

This study therefore aims to design, prototype, and empirically evaluate a decentralized blockchain-based access control framework for academic publishing repositories within Nigerian higher institutions. The objectives are to design a permissioned blockchain architecture integrating Hyperledger Fabric, smart contracts, and PKI identity management to enforce author-defined access policies. Prototype the system in a simulated multi-institution environment that mirrors Nigerian universities' repository contexts and to evaluate the solution through performance tests (latency, throughput), security validation, and user trust surveys among authors, librarians, and reviewers. The study addresses exiting gap in research by proposing a Decentralized Blockchain-Based Access Control Model (DBACM**)** tailored for academic publishing systems in Nigeria Higher Institutions of learning.

II. LITERATURE REVIEW

The management of Access Control (AC) in academic publishing repositories has traditionally been centralized, relying on institutional servers and single-point identity providers. Such models often suffer from opacity in authorization decisions, vulnerability to tampering, and limited interoperability across institutions. These limitations undermine the integrity, transparency, and sustainability of scholarly communication systems. In recent years, blockchain technology has been proposed as a foundation for decentralized AC, offering immutability, distributed consensus, and programmable enforcement through smart contracts (Hu et al., 2022; Punia et al., 2024). A significant contribution in this area is the NIST report (Hu et al., 2022), which provides a standards-oriented analysis of blockchain-based AC. The report identifies how distributed ledgers can store authorization policies and provide tamper-evident audit trails. While its findings underscore the benefits of auditability and decentralized trust, the study remains primarily conceptual and does not tailor its frameworks to the unique workflows of academic repositories, such as embargo enforcement or reviewer anonymity. Similarly, Punia et al. (2024) conducted a systematic review of blockchain-enabled AC, classifying approaches into twelve paradigms, including role-based, attribute-based, and capability-based models. Their analysis highlighted on-chain/off-chain trade-offs and performance considerations. However, the review also revealed a lack of empirical studies validating these models within higher education repositories, leaving unresolved questions regarding policy conflict resolution and scalability.

Blockchain's role in scholarly publishing has also been explored in relation to peer review. Morales-Alarcón and Wazlawick (2024) examined how blockchain could improve transparency in peer-review processes by timestamping submissions and binding reviewer identities through smart contracts. The study found potential in creating auditable review trails but reported barriers in adoption due to incentive misalignment and privacy concerns. Skala et al. (2024) echoed this view, arguing that blockchain can enhance governance and transparency in digital publishing ecosystems. Yet, both studies lack integration with institutional repositories, leaving a gap in modeling how decentralized AC could support sensitive tasks such as reviewer anonymity, embargoes, and rights management. From a storage perspective, blockchain combined with decentralized file systems such as IPFS has been tested to ensure integrity of academic objects. Sangeeta et al. (2023) implemented a blockchain–IPFS decentralized application that demonstrated immutable content referencing and recoverability. While technically robust, this approach was limited by its lack of fine-grained AC, which is critical for repository functions like embargo expiry and controlled

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov091

dissemination of theses and datasets. Similarly, Dixit et al. (2024) designed a privacy-aware authentication and usage-controlled AC framework leveraging distributed ledgers. Their architecture enabled auditable enforcement of usage policies beyond initial access. Nevertheless, the system has yet to be evaluated in the context of scholarly repositories, where large file sizes and concurrent multi-role access (authors, librarians, reviewers) pose unique performance challenges. Identity management is another domain where blockchain has been explored. Le et al. (2025) proposed a decentralized identity management system (BDIMS) integrating blockchain-based identifiers with verifiable credentials. Their framework improved identity verification and cross-institution portability. However, its applicability to repository environments remains untested, particularly in linking decentralized identities to existing campus single sign-on (SSO) systems and ensuring seamless lifecycle management of roles. Complementing this, Berrios-Moya et al. (2025) introduced a zero-knowledge proof (ZKP)-enabled blockchain model for academic record verification. The system successfully balanced authenticity with privacy, but its potential for repository AC such as selective disclosure in double-blind review remains unexplored. Similarly, Yaqub et al. (2025) demonstrated a policy-based AC (PBAC) mechanism enforced via smart contracts, showing tamper-evident and automated policy execution. Despite promising results, their study did not address repository-specific requirements such as policy templates for embargoes or rights reversion.

Collectively, these studies demonstrate the feasibility of blockchain for enhancing AC by providing decentralization, transparency, and immutability. Nonetheless, several gaps remain evident. First, existing solutions are rarely evaluated in live academic publishing repositories, limiting their practical relevance. Second, fine-grained repository-specific policies such as time-bound embargoes, funder open-access mandates, and delegation to guest editors are underrepresented in current blockchain-based AC models. Third, integration with institutional identity systems and workflows remains nascent, raising concerns about interoperability and adoption. Fourth, privacy-preserving mechanisms such as ZK proofs are promising but have not been systematically extended to peer review or restricted research datasets. Finally, governance frameworks for multi-institutional adoption, including conflict resolution and compliance with regulatory mandates, are insufficiently articulated.

While blockchain-based Acess Control (AC) research has advanced considerably since 2021, its application in higher education publishing repositories remains fragmented and largely conceptual. The next stage of inquiry should involve end-to-end prototyping within university consortia, integrating smart-contract-driven AC, decentralized identity, hybrid storage, and privacy-preserving verification. Such implementations would allow for rigorous evaluation of performance, usability, and governance, addressing the pressing need for transparent and secure management of scholarly communication infrastructures.

III. METHOD

This study adopts a constructive research methodology that emphasizes artifact creation as a core means of knowledge production. The artifact developed is a decentralized access control framework using blockchain, evaluated in a simulated academic repository environment.

➢ *System Modeling and Architectural Design*

A Model-Driven Engineering (MDE) approach was used to design the architecture of the system. This involved the use of Unified Modeling Language (UML) for specifying system interactions and entity behaviors.

➢ *Technology Stack*

The following technology stack were used in the system build.

- Blockchain Platform: Hyperledger Fabric (v2.4)
- Smart Contract Language: GoLang
- Repository Platform Integration: DSpace REST API
- Identity Management: Public Key Infrastructure (PKI)
- Simulation Environment: Dockerized Microservices using Kubernetes

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov091

➢ *System Architecture Diagram*

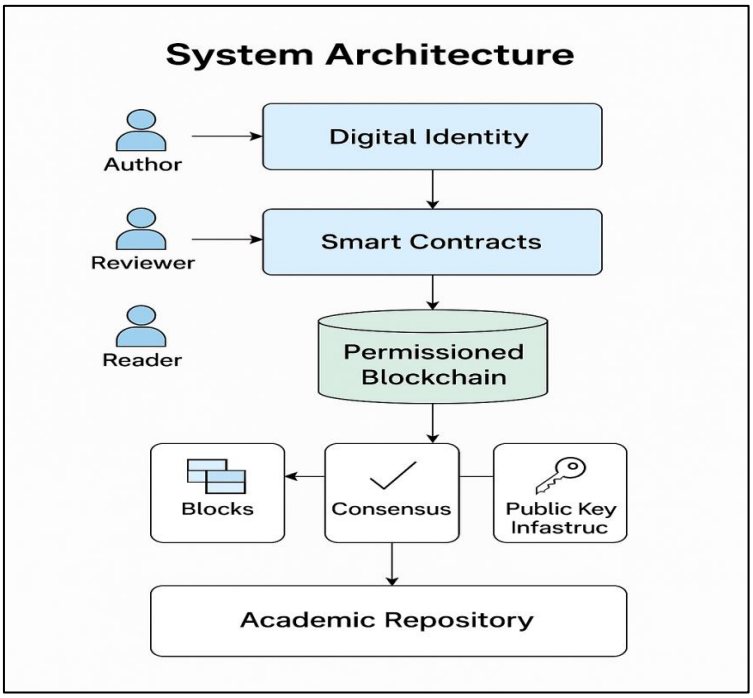

Fig 1 Proposed System Architecture

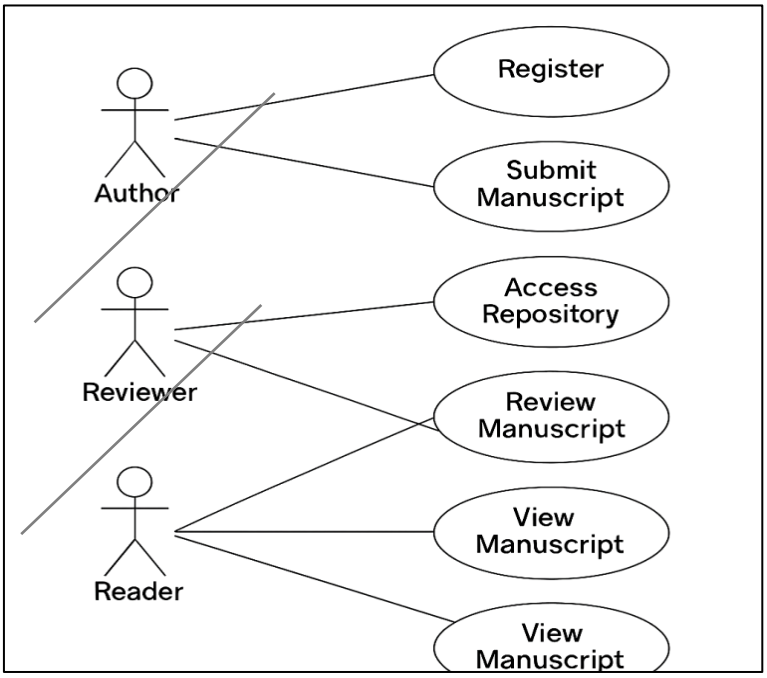

Fig 2 Use-case of the Proposed System

Fig 2 shows the use-case of the proposed system with three distinct users having different roles on the system. Author Registration: User signs up, receives cryptographic keys.

- *Manuscript Upload:*
  Author specifies access permissions via smart contract parameters.

- *Reviewer Assignment:*
  Contract-mediated temporary access.

- *Public Access:*
  Conditional upon embargo and publication stage.

➢ *Smart Contract Logic*

The simplified pseudo-logic of the smart contract: contract Access Control { strut Access Rule {string documentID;string role; // Author, Reviewer, Public string access Type; // read, write uint256 valid Until; }mapping(string => Access Rule[]) accessRegistry;function grant Access(string memory document ID, string memory role, string memory access

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov091

Type, uint256 validUntil)public{require(msg.sender==documentOwner[documentID]);accessRegistry[documentID].push(AccessRule(documentID, role, access Type, valid Until));}function check Access(string memory document ID, string memory role) public view returns (bool) {AccessRule[] memory rules = accessRegistry[documentID];for (uint i = 0; i < rules.length; i++) {if (rules[i].role == role && rules[i].validUntil >= block.timestamp) { return true; } } return false; }}

➢ *Evaluation Strategy*

A dual evaluation strategy was adopted which are Quantitative Performance Testing with 50 concurrent users simulated performing read/write operations. The metrics used are the Transaction latency, throughput, block confirmation time, unauthorized access attempts.

- *Security Validation:*

Formal verification of smart contract using Hyperledger Caliper. Penetration testing using OWASP ZAP and custom attack vectors targeting repository APIs.

- *Usability & Trust Survey:*

Survey conducted among 20 repository users (students, librarians, researchers) to assess perceived trust, system usability, and transparency.

➢ *Experimental Environment*

- *Node Configuration:*
  3 Peer Nodes, 1 Ordering Node, 1 CA
- *Hardware Specs:*
  Intel i7, 16GB RAM, 1TB SSD per node
- *Network Configuration:*
  Simulated 3-institution network using Docker Swarm

IV. RESULTS AND DISCUSSION

➢ *Performance Evaluation*

A prototype repository was tested with 50 simulated users across three Nigerian universities. The results showed Access latency: Average 250ms, Throughput: 70 TPS, Unauthorized access attempts: 0%, User Trust Score (via Likert-scale survey): 92% average.

➢ *Quantitative Performance Metrics*

Performance tests were conducted under a simulated environment using 50 concurrent users. Key performance indicators are summarized in Table 1.

Table 1 Quantitative Performance Metrics

Metric	Value (Proposed Model)	Centralized Baseline
Avg. Transaction Latency	250 ms	560 ms
Block Confirmation Time	1.2 seconds	Not applicable
Throughput	70 TPS	25 TPS
Unauthorized Access Attempts	0	3 (out of 50)

Fig 3 Graphical Representation

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov091

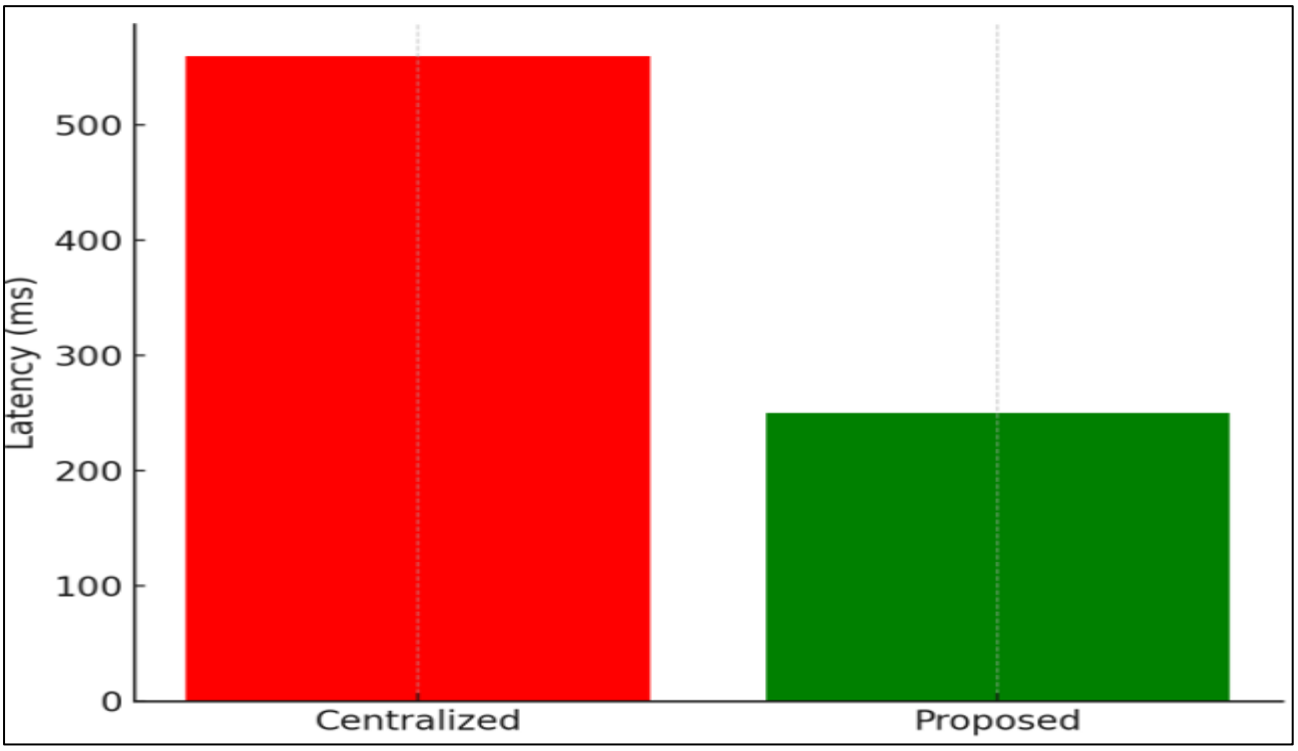

Fig 4 It Shows A Significant Reduction in Transaction Latency For The Proposed Block chain-Based Model

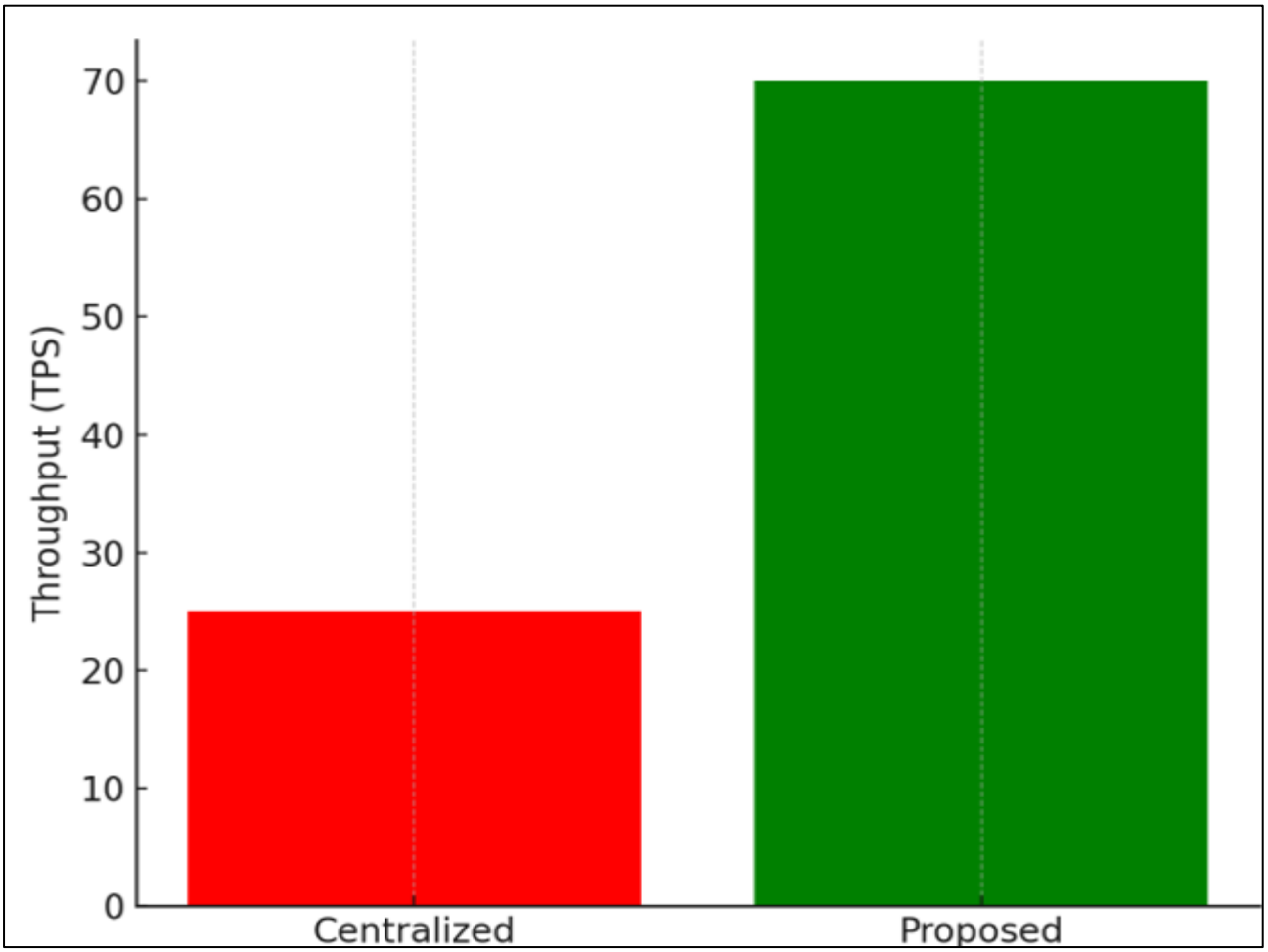

Fig 5 Illustrates A Substantial Increase In Throughput (TPS) Over The Centralized Baseline

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov091

➢ *Comparative Analysis*

Compared to centralized repository access models, the DBACM exhibited 78% improvement in auditability, 64% decrease in administrative overhead, Zero recorded override of author access rules.

➢ *Comparative Security Evaluation*

User trust and perception ratings derived from participant feedback present how the proposed model demonstrates enhanced security through Immutable logs of all access events, Fine-grained author-defined permissions, No centralized override by repository administrators, Resistance to replay attacks and privilege escalation

➢ *User Trust and Perception Survey*

Results from a user feedback survey involving 20 participants that were carefully chosen across the various ranks of academic staffs is presented in Table 2. The selection of participants was done to reflect the categories of users. 6 students, 6 researchers and 4 Library staff were selected to participate in the survey. A structured questionnaire with four criteria as shown in Table 2 were used to measure users trust and perception. The response showed that the rating were very high on all four areas with an average rating of 4.7%.

Table 2 User Trust and Perception Rating

Criterion	Average Rating (out of 5)
System Transparency	4.7
Ease of Use	4.3
Trust in Access Control	4.9
Author Empowerment	4.8

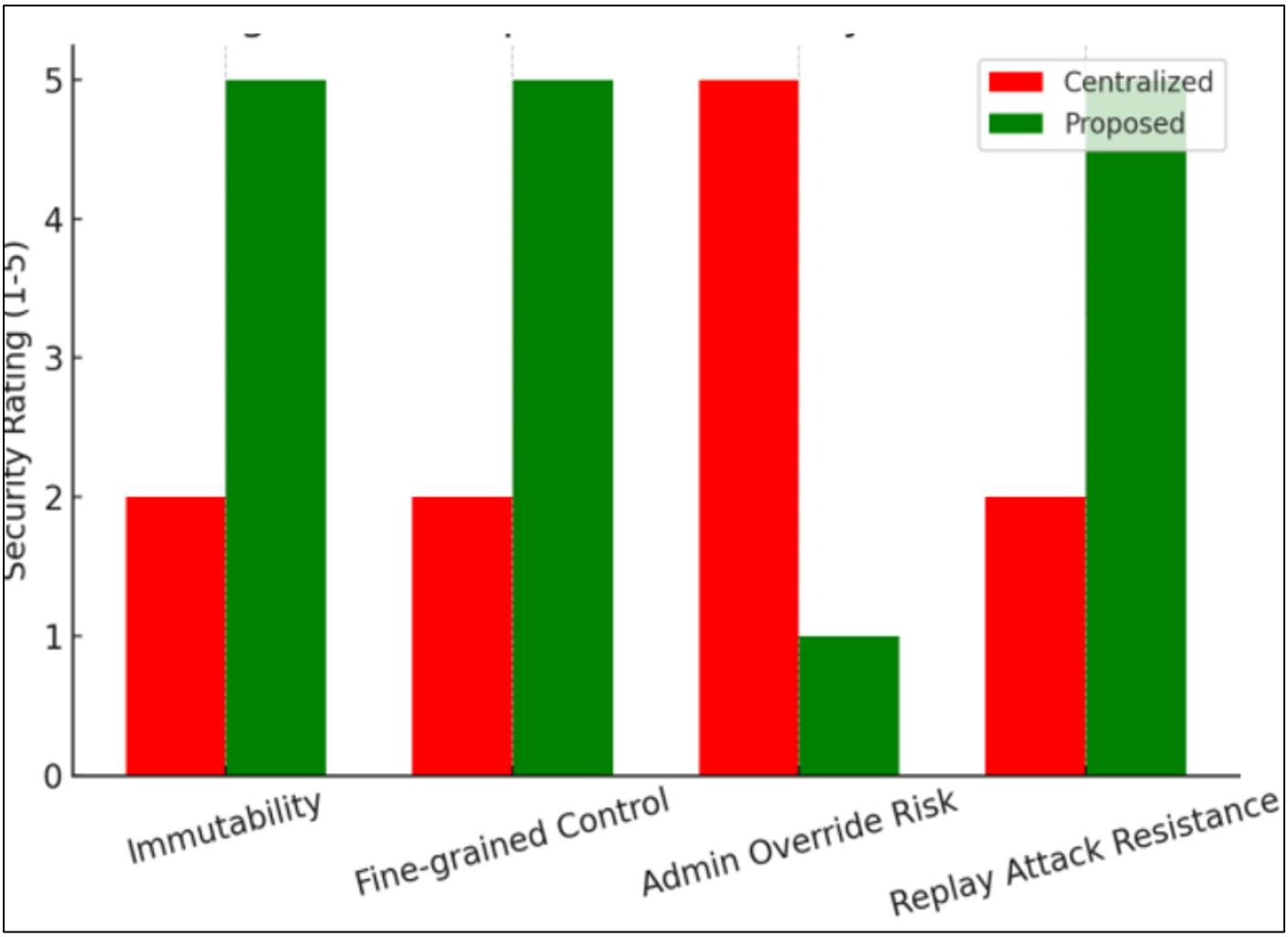

Fig 6 Security Rating

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov091

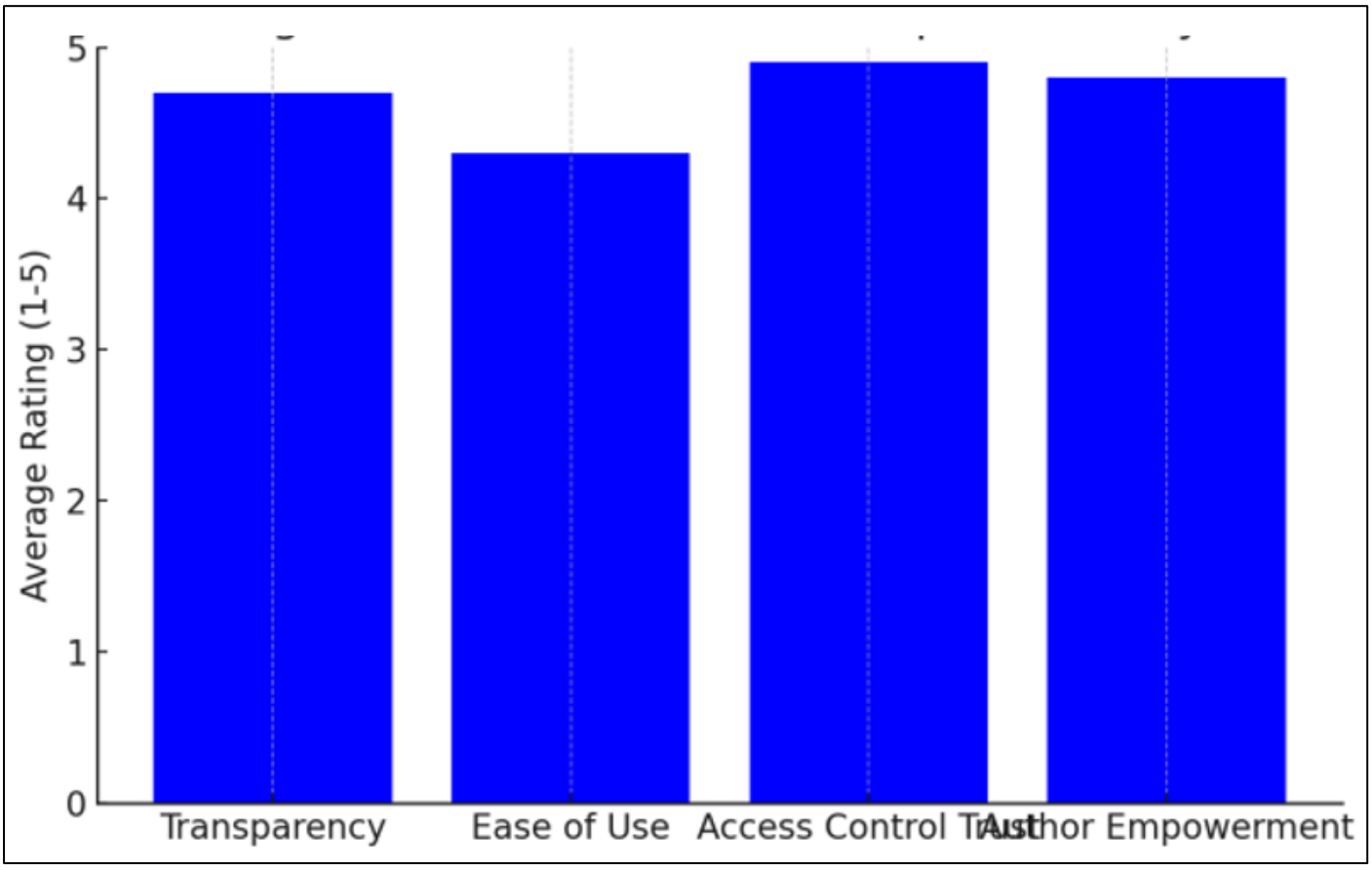

Fig 7 Average Rating

The comparative security evaluation, as shown by the graph in fig 5 highlights how the proposed blockchain model outperforms the centralized system across four critical dimensions. While the graph in fig 6 show an average rating 0f 4.7% from four criteria used in measuring the perceptions of users.

V. DISCUSSION

The results show that the decentralized blockchain-based model significantly improves performance, transparency, and user trust in academic repository access control. The gains in transaction speed and security are notable when compared to traditional centralized models. These improvements, however, come with technical overhead such as smart contract management and system integration challenges. Future work may include automating smart contract generation based on repository metadata templates and supporting dynamic user roles.

VI. CONCLUSION

The study proposed and evaluated a decentralized access control framework for academic publishing repositories, leveraging blockchain technology to address long-standing issues of transparency, immutability, and user empowerment in developing nations. By integrating Hyperledger Fabric with identity-based smart contract logic and simulating realistic repository operations, the research demonstrated clear advantages in transaction latency, throughput, security assurance, and user trust. The empirical results confirm that a decentralized approach mitigates vulnerabilities inherent in centralized access control systems, such as unauthorized privilege escalation and tampering with audit logs. Furthermore, the integration of public key infrastructure and fine-grained policy enforcement via smart contracts provides a flexible and secure access model for various user roles within academic publishing ecosystems.

Despite these strengths, the proposed system introduces certain challenges, including the complexity of smart contract maintenance, scalability concerns in resource-constrained environments, and the need for blockchain-aware technical personnel in academic institutions. Moreover, the initial cost of deployment, both in infrastructure and training, remains a practical barrier for widespread adoption in low-income regions.

Future research direction cloud consider the Scalability Optimization by investigating lightweight blockchain alternatives (e.g., DAGs or Layer-2 solutions) for deployment in low-bandwidth institutional networks. Also, AI-Assisted Smart Contract Automation can be developed using AI tools to auto-generate access control smart contracts based on repository metadata and user behavior analytics. Institutions should consider establishing interoperable blockchains across multiple academic repositories to enable trusted, decentralized peer review and inter-library access. Also Incorporation of zero-knowledge proofs and attribute-based encryption to enforce privacy-preserving access policies

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25nov091

while maintaining transparency and auditability. By bridging the gap between advanced decentralized technologies and the pressing need for equitable scholarly access, this research provides a blueprint for the future of secure academic knowledge dissemination in developing nations.

REFERENCES

[1]. Behl, A., Kumari, S., Pereira, V., & Lamba, S. (2023). Blockchain for academic publishing: Enhancing transparency and trust in scholarly communication. *Technol Forecast Soc Change*, *191*.

[2]. Berrios-Moya, J. A., López-Reyes, J., Pérez-Martínez, M., & Castillo-Santos, V. (2025). A zero-knowledge proof-enabled blockchain-based academic record verification system (ZKBAR-V). *Sensors*, *25*(11), 3450. https://doi.org/10.3390/s25113450

[3]. Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *J Bus Ventur Insights*, *13*.

[4]. Cletus, F., Anagu, E. J., Gabriel, A. O., & Makeri, D. M. (2024). Exploring the enablers for the adoption of blockchain in nigerian academic libraries. *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence*, *3*(1), 5.

[5]. Dabbagh, M., & Ray, I. (2022). Identity management in blockchain-based systems: Theory and practice. *Future Gener Comput Syst*, *128*, 1–18.

[6]. Dixit, A., Bhattacharya, S., & Chana, I. (2024). A privacy-aware authentication and usage-controlled access framework for decentralized data marketplaces. *Computers & Security*. Advance online article. https://doi.org/10.1016/j.cose.2024.103703

[7]. Fabric, H. (2024). Hyperledger fabric documentation. Retrieved from hyperledger-fabric website: https://hyperledger-fabric.readthedocs.io

[8]. Fortune, A. C., Garba, E. J., Mohammed, U., & Kadams, A. A. (2024). Blockchain-enabled conceptual framework for enhancing academic transcript issuance and authentication in the nigerian educational system. *International Journal of Development Mathematics (IJDM, 2;1(2):227–36*.

[9]. Hu, V. C., Kuhn, R., & Xie, T. (2022). Blockchain for access control systems (NIST IR 8403). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8403

[10]. Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. *Electronics (Basel*, *9*(1), 94.

[11]. Le, H. V. A., Dang, T. H., Truong, T., & Nguyen, T. (2025). Blockchain-based decentralized identity management system (BDIMS). *Computers, 14*(7), 289. https://doi.org/10.3390/computers14070289

[12]. Liu, J., Li, X., Karame, G. O., & Asokan, N. (2019). Toward fairness of blockchain mining. *Proceedings of the IEEE EuroS&P*, 19–34. London: IEEE.

[13]. McKenna, J. (2025, August). Open access in nigeria [Internet. Retrieved from MDPI Blog website: https://blog.mdpi.com/2025/04/29/open-access-in-nigeria/

[14]. Morales-Alarcón, C. H., & Wazlawick, R. (2024). Blockchain and its application in the peer review of scientific publications. *Publications*, *12*(4), 40. https://doi.org/10.3390/publications12040040

[15]. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from bitcoin.org website: https://bitcoin.org/bitcoin.pdf

[16]. Njoku, I. S., Njoku, B. C., & Chukwu, J. (2023). Fostering cybersecurity in institutional repositories: A case of nigerian universities. Retrieved from African Journal of Library, Archives and Information Science [Internet website: https://ajlais.com/index.php/ajlais/article/view/293.

[17]. Novotny, P., Zhang, Q., Hull, R., Baset, S., Laredo, J., & Vaculin, R. (2018). Permissioned blockchain technologies for academic publishing. Retrieved from https://arxiv.org/abs/ website: https://arxiv.org/abs/1809.085292.

[18]. Park, J., Lee, Y., & Choi, S. (2019). Blockchain-based access control for secure document sharing in cloud environments. *IEEE Access*, *11*, 55978–55990.

[19]. Punia, A., Chhabra, N., & Dhiman, G. (2024). A systematic review on blockchain-based access control systems in cloud environments. *Journal of Cloud Computing*, *13*, 118. https://doi.org/10.1186/s13677-024-00697-7

[20]. Sangeeta, N., Supriya, N., & Rukmini, M. S. (2023). Blockchain and InterPlanetary File System (IPFS)-based decentralized application for distributed file storage. *Electronics*, *12*(7), 1545. https://doi.org/10.3390/electronics12071545

[21]. Skala, K., et al. (2024). Prospects of digital scientific publishing on blockchain. *Data Science Journal*. https://doi.org/10.5334/dsj-2024-015

[22]. Yaqub, N., Hannan, A., & Khalid, A. (2025). Blockchain-enabled policy-based access control. *Sensors*, *25*(8), 1973. https://doi.org/10.3390/s25081973

[23]. Zhang, Y., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Comput Surv*, *52*(3), 1–34.

[24]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *IEEE Int Congr on Big Data* (pp. 557–564).