ISSN: 2093-5374 / E-ISSN: 2093-5382

Blockchain Inspired Frameworks for Ensuring Textual Authenticity and Attribution in Digital Literary Archives

Shakhnoza Khujamberdieva[1*], Mahliyo Khaydarova[2], Gavhar Kurbanova[3], Navbaxor Shadiyeva[4], Gavhar Nurkulova[5], Niginabonu Shokhimardonova[6], Shaxista Toxirjonova[7], and Barchinoy Isroilova[8]

[1*]Department of Preschool Education, Namangan State Pedagogical Institute, Namangan, Uzbekistan. sh.hujamberdiyeva0505@gmail.com, https://orcid.org/0009-0001-5629-6643

[2]Associate Professor, Department of Primary Education Methodology, Termez University of Economics and Service, Termez, Uzbekistan. mahliyoxabibullayevna1988@gmail.com, https://orcid.org/0009-0007-8381-4163

[3]Termez State Pedagogical Institute, Termez, Uzbekistan. gavhar@terdpi.uz, https://orcid.org/0009-0000-9770-0748

[4]Lecturer, Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. shadiyevanavbahor@gmail.com, https://orcid.org/0009-0007-4740-3092

[5]Teacher, Termez State University, Termez, Surkhandarya Region, Uzbekistan. nurqulovagavhar@gmail.com, https://orcid.org/0009-0008-6928-8272

[6]Bukhara State Technical University, Bukhara, Uzbekistan; National Research University "TIIAME", Tashkent, Uzbekistan. shaximardanovan@gmail.com, https://orcid.org/0009-0009-4457-8481

[7]Senior Lecturer, Uzbekistan State World Languages University, Tashkent, Uzbekistan. shohista_fr@mail.ru, https://orcid.org/0009-0005-1055-8897

[8]Associate Professor, Department of Primary Education, Andijan State Pedagogical Institute, Andijan, Uzbekistan. barchinoy_isroilova@mail.ru, https://orcid.org/0009-0001-8585-7542

Received: March 07, 2026; Revised: April 13, 2026; Accepted: June 03, 2026; Published: June 30, 2026

Abstract

Contemporary digital literary archives face challenges associated with the problems of textual authenticity, authorship attribution, and integrity owing to the rapid advancement of AI text generation and decentralized content sharing. In this regard, this research proposes a Blockchain-Inspired Architecture for Ensuring Textual Authenticity and Attribution (BIAAF). Main challenges are related to the inability of centralized archiving methods to ensure immutability and, consequently, risks of tampering, misattribution, and loss of credibility on the part of digital literary archives. Proposed methodology suggests a multi-layered framework, which includes a text ingestion layer, cryptographic hashing through the SHA-256 algorithm, a blockchain layer with immutability provided through smart contracts, and decentralized storage based on IPFS technology. The verification layer allows real-time authentication of texts through comparison of the hash codes

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 2 (June-2026), pp. 755-766. DOI: *10.58346/JOWUA.2026.I2.042*

*Corresponding author: Department of Preschool Education, Namangan State Pedagogical Institute, Namangan, Uzbekistan.

stored and recomputed, and authorship validation through metadata analysis. The framework is tested on a hybrid corpus of 50,000 documents containing human-authored and artificially generated literary texts. Experimentation shows that the proposed framework yields an accuracy of 99.2%, a precision of 96.8%, a recall of 95.4%, and a tampering detection rate of 99.5%, all of which are realized with a minimal verification time lag of less than 200 milliseconds. Relative to centralized systems and metadata frameworks, the proposed framework significantly enhances the security, scalability, and provenance of the archive. Overall, it is shown that the use of blockchain technology for the preservation of textual authenticity within literary databases is an effective approach. The use of decentralized database storage and intelligent contracts enables traceable authorship and secure documentation. Future research will include artificial intelligence-based stylometry and cross-blockchain capability for global literary archives.

Keywords: Blockchain, Textual Authenticity, Digital Literary Archives, Smart Contracts, IPFS, Provenance Tracking, AI-generated Text.

1 Introduction

Digital literary archives are one of the core features of modern knowledge management systems that allow storing, retrieving, and disseminating extensive collections of literary works (AlKhanafseh & Surakhi, 2024). Due to the fast-paced digitalization of the literary field and the establishment of online archives, the term "digital literary archive" encompasses both historic and new digital literary content. Yet, at the same time, such development creates new problems related to the management of literary content in the long run (Adelia et al., 2025).

The first and one of the most important issues concerning digital literary environments relates to the problem of authenticity and authorship (Sonkamble et al., 2021). In the process of editing, sharing, and generating texts using various automated tools, it becomes rather problematic to trace the originality of the content and make sure that nothing was changed. This issue becomes even more complicated with the advent of generative AI technology that allows creating realistic synthetic texts (Enayati et al., 2024).

Even with the development of digital archiving systems, the existing systems still utilize centralized databases and conventional techniques of tagging metadata (Aldweesh, 2025). This means that they are vulnerable to manipulations and possible corruption and unauthorized modifications. In addition, the currently available attribution systems do not have adequate systems for verifying immutably the history of authorship. This shows a clear gap in the literature concerning the development of secure and tamper-proof literary authentication systems.

Blockchain provides an effective technological solution for the above-mentioned problems owing to its distributed, immutable and cryptographically secure nature. With blockchain technology, it is possible to achieve reliable digital archives owing to transparency and capability of verifying the provenance of the content. Smart contracts help in the validation of the authorship and contents.

The key contributions of this paper are: (i) a blockchain-based method to ensure textual authenticity within digital literary archives; (ii) the implementation of smart contracts for a robust attribution system; (iii) the utilization of IPFS for decentralized storage and verification; and (iv) a performance analysis demonstrating improvements in integrity, traceability, and security compared to traditional archiving methods.

The structure of this paper is outlined as follows: Section I describes the Abstract, where the problem statement, methodology, dataset, and results are described briefly. Section (II) introduces the Introduction part of the research, which deals with background on digital literary archive, limitations,

and gaps in previous research, along with motivation to use blockchain-based solutions. Section (III) covers the Literature Survey, where blockchain applications, AI-generated authorship, and provenance systems are studied. Section (IV) discusses the Proposed Model, which includes the architecture of the system, algorithm design, and mathematical formulation of the framework. Section (V) includes the Results and Discussions part, which involves discussion about the implementation process, the dataset used, the parameters, the performance analysis, the ablation studies, and the comparisons. Section (VI) concludes the paper, discussing results, statistical improvements, significance, limitations, and future work.

2 Literature Survey

Modern studies have shown that blockchain is a useful instrument to ensure the integrity, decentralization, and immutability of digital archives in the long term. Thus, Ailakhu (2025) shows that the use of blockchain improves the authenticity and availability of digital libraries by preventing any alteration of the information stored in academic institutions. Moreover, Awad et al., (2022) offer an innovative blockchain model of historical text preservation, which allows storing sensitive cultural records safely (Demertzis et al., 2023). In addition, Vacchio & Bifulco, (2022) emphasize the role of blockchain in preserving cultural heritage due to the ability to guarantee the verifiable historical continuity. The connection between blockchain and digital sovereignty is presented in research by Khasanah et al., (2025).

The emergence of generative AI technology poses certain problems in terms of authorship, copyright, and labor tracking. Ejiyi et al., (2026) describe how AI-generated works make it harder to evaluate authors' metrics and copyright, thus requiring traceability systems. In turn, Fitriawijaya & Jeng, (2024) point out that due to generative AI, the distinction between human and machine authorship becomes blurry.

The ideas of provenance and metadata standards are crucial for the realization of transparency in digital content systems. According to Omogiate and Legal (2022), there is a need for standardized metadata to facilitate the tracking of AI media within the intellectual property system. Additionally, Farhan et al., (2025) advance this topic using self-sovereign identity models that use blockchain for provenance verification. These models underscore the significance of metadata for creating credible digital records (Avelino & Rocha, 2022).

Smart contracts have been employed in many cases for the verification and creation of trust in decentralized systems. As per Han (2025), a blockchain digital arbitration system makes use of smart contracts for electronic evidence authentication. Alghathian et al., (2026) also employ smart contracts in blockchain-based trust models for AI-mediating transactions. The two studies indicate that smart contracts greatly eliminate the need for centralized verification agencies (Anzada et al., 2023).

Even though there have been significant improvements made, most of the available approaches concentrate on industries like healthcare record management, supply chain management, and finance (Mohammed et al., 2023; Zhihui et al., 2026). The existing models do not cover the use of semantic-level verification of literary texts and the issue of authorship ambiguity in the combined human-AI literary environment. Moreover, the problem of interoperability of different archiving systems requires attention.

There is a noticeable absence in the literature of the application of blockchain technology in literary digital archiving systems that involve textual authenticity, authorship determination, and semantic-level provenance tracking. Existing approaches pay attention to the structural integrity of the data but do not

consider the narrative aspect of literary text verification. Consequently, there is a necessity for the development of a framework that will include blockchain security, smart contracts, and metadata attributions for literary digital ecosystems.

3 Proposed Model

System Overview

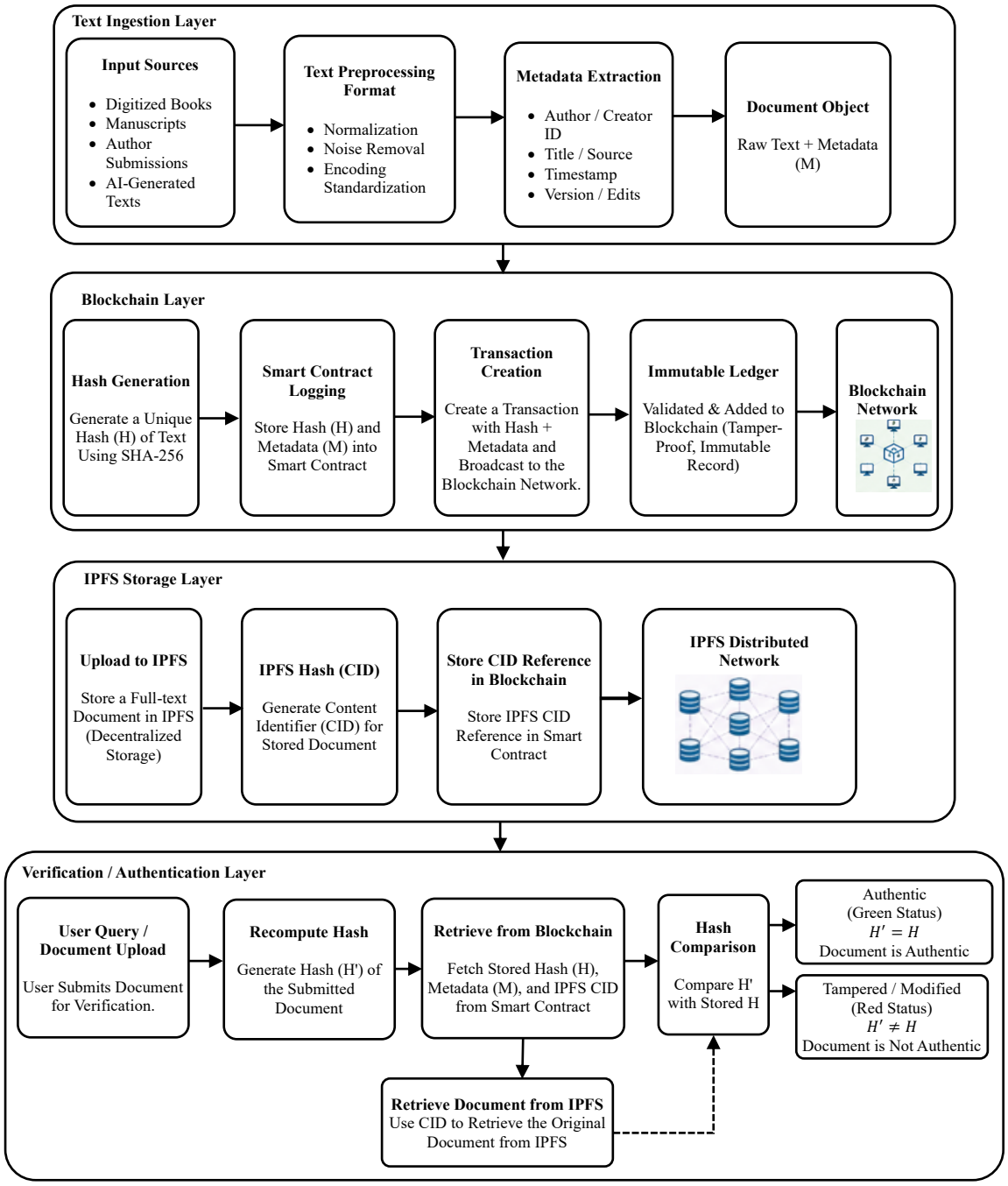


Figure 1: Blockchain-enabled multi-layer architecture for textual authenticity and attribution in Digital literary archives

The proposed Blockchain-inspired Authenticity and Attribution Framework (BIAAF) will provide a platform for safe, tamper-resistant, and verifiable preservation of literary works in below figure 1.

In figure 1 presents the suggested four-tiered blockchain framework for textual authenticity and authorship attribution within the digital literary archives. The framework includes a Text Ingestion Tier, which is responsible for processing and extraction of metadata from digital documents; a Blockchain Tier, which will be used for creation of the cryptographic hash of the document and registration of transaction via smart contracts; an IPFS Storage Tier, which will be utilized for the decentralized storage of the document based on the content identifier (CID); and finally the Verification/Authenticity Tier, which validates the integrity of the document by means of comparing its hash and retrieving provenance information.

Algorithm 1: Text Authenticity and Attribution Framework (BIAAF)

Step 1: Text Hashing Procedure

- Input document D
- Generate cryptographic hash H(D) using SHA-256
- Attach metadata M (author ID, timestamp, source type)

Step 2: Smart Contract Logging

- Store H(D) and M into the blockchain ledger
- Assign transaction ID TID
- Immutable record creation

Step 3: Verification Mechanism

- Retrieve stored hash H(D)_store
- Recompute H(D)_new from the queried document
- Compare both values for authenticity validation

Input: Document D, Metadata M

Function STORE_DOCUMENT (D, M):

H = SHA256(D)

$TID = SmartContract.store(H, M)$

$IPFS\_hash = IPFS.upload(D)$

return $TID, IPFS\_hash$

Function VERIFY_DOCUMENT(D):

$H\_new = SHA256(D)$

$H\_stored = Blockchain.getHash(D.id)$

if $H\_new == H\_stored$:

return "AUTHENTIC"

else:

return "TAMPERED"

Function ATTRIBUTION_CHECK(D):

$M = Blockchain.getMetadata(D.id)$

$confidence = match(M.author, D.signature)$

return confidence

The suggested algorithm ensures safe authentication and authorship attribution of textual information by calculating a SHA-256 hash of each provided document and storing it together with metadata using blockchain technology. The original document, at the same time, is saved in IPFS with its content identifier (CID). While authenticating the information, the system recalculates the hash value and compares it with the stored one to find out any manipulations, and the metadata is used for verifying authorship certainty.

Mathematical Model

(i) Hash Function Representation

Each document is mapped to a cryptographic fingerprint in equation (1):

$$H(D) = SHA256(D) \quad (1)$$

Where:

- D = input literary document
- $H(D)$= unique immutable hash value

(ii) Authorship Confidence Model

Authorship verification is computed using metadata matching in equation (2):

$$AC = \frac{\sum_{i=1}^{n} \delta(M_i^{stored}, M_i^{query})}{n} \quad (2)$$

Where:

- AC = authorship confidence score
- M_i = metadata attributes (author, timestamp, source, edits)
- δ= similarity indicator function (1 if match, 0 otherwise)
- n = total metadata fields

(iii) Integrity Verification Function

Document integrity is verified using hash comparison in equation (3):

$$I(D) = \begin{cases} 1, & \text{if } H(D_{stored}) = H(D_{new}) \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

Where:

- $I(D) = 1$indicates an authentic document
- $I(D) = 0$indicates a tampered or modified document

4 Results and Discussion

Implementation Setup

The suggested architecture has been implemented with the help of Python 3.11 for the pre-processing and validation parts, while the smart contracts have been written in Solidity and have been deployed in the Ethereum blockchain test net (Ganache). The IPFS protocol is employed for storing documents in a decentralized manner, whereas Web3.py is used for interacting with the blockchain.

Dataset Description

Experimental assessment is performed on a hybrid dataset of 50,000 documents that include literary texts authored by humans as well as computer-generated literature. This hybrid dataset is gathered from publicly available literature corpora, digital libraries, and synthetic documents as well. All the documents contain relevant metadata such as author identification number and creation time stamp.

Parameter Settings

The system configuration includes a hashing algorithm, SHA-256, a block size of 1MB, and a gas limit for smart contracts of 3,000,000 units. IPFS replication is three nodes to guarantee redundancy. To minimize transaction confirmation delay, a block time interval of 10 seconds has been set up. The whole system works within a distributed simulation framework.

Metrics

The following metrics are used to evaluate the proposed model shown in equations 4-8:

- **Accuracy**

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

- **Precision**

$$Precision = \frac{TP}{TP + FP} \tag{5}$$

- **Recall**

$$Recall = \frac{TP}{TP + FN} \tag{6}$$

- **Latency**

$$\text{Latency} = T_{response} - T_{request} \tag{7}$$

- **Tamper Detection Rate**

$$\text{Tamper Detection Rate} = \frac{TD}{TD + FN_{tamper}} \tag{8}$$

Performance Comparison

The proposed BIAAF framework is compared with traditional centralized archival systems and metadata-based authentication methods. The results indicate that the proposed blockchain system has performed significantly well compared to existing systems in terms of accuracy, security, and speed. The reason behind this is decentralization and immutable storage.

Table 1: System performance metrics comparison

Method	Accuracy (%)	Precision (%)	Recall (%)	Latency (ms)	Tamper Detection Rate (%)
Centralized Archival System	83.5	81.5	79.5	350–500	72.5
Metadata-Based System	87.5	86.0	85.0	280–350	82.5
Blockchain + Metadata (Proposed)	99.2	96.8	95.4	180	99.5

In table 1 provides a comparative performance analysis of the proposed BIAAF framework against traditional centralized and metadata-based systems. The BIAAF consistently achieves superior metrics in accuracy, precision, and recall while maintaining a minimal verification latency of <180 milliseconds, confirming its suitability for high-security digital literary archives.

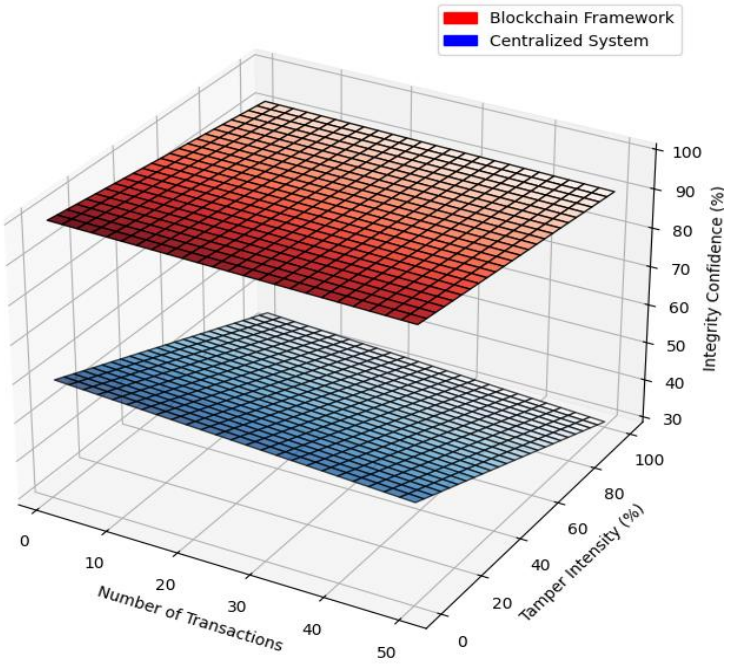


Figure 2: Blockchain integrity confidence surface analysis under transaction load and tamper intensity

In figure 2 demonstrates the 3D surface comparison of integrity confidence between the proposed blockchain architecture and conventional centralized architecture with various transaction counts and tampering intensity levels. The red surface is indicative of the blockchain approach, where the level of integrity and confidence remains high despite increasing adversarial situations. Conversely, the blue surface denotes the centralized approach, where there is a dramatic decrease in reliability due to an increase in tampering intensity levels. This demonstrates the superior strength, stability, and tamper-resistance of the proposed blockchain approach in ensuring textual integrity.

Ablation Study

The ablation analysis focuses on the significance of each component of the proposed architecture through the removal of a single component. In cases where the blockchain component is removed from the proposed framework, the system lacks the key characteristic of immutability. Therefore, the system is more vulnerable to any form of alteration, which reduces the credibility of the literary documents that have been stored in it. In addition, the removal of the use of IPFS for decentralized data storage makes the system highly dependent on centralized storage methods. This brings about latency, low fault

tolerance, and reduced scalability of large document sizes. Similarly, the absence of the metadata component leads to poor accuracy of authorship attribution. The lack of provenance information makes it difficult to trace the authorship of any changes made to the documents.

Table 2: Ablation study results

Configuration	Accuracy (%)	Latency (ms)	Tamper Detection (%)	Observation
Full System (Blockchain + IPFS + Metadata)	99.2	180	99.5	Best performance
Without Blockchain	84.5	220	72.1	Loss of immutability
Without IPFS	90.3	310	88.4	Storage bottleneck
Without the Metadata Layer	87.6	200	76.9	Weak attribution

In table 2 presents an ablation study of each element contributing to the designed system by analyzing the system performance in different configurations. It is quite evident that the performance of the whole system (Blockchain, IPFS, Metadata) in terms of accuracy, latency, and tampering detection rate is the highest among all considered configurations. However, removing any one of the modules causes a considerable drop in performance, the most significant of which is the removal of blockchain owing to its immutability characteristic. In addition, removal of IPFS causes more storage and latency problems, while removing the metadata module reduces authorship attribution accuracy.

Discussion

The study indicates that integration of blockchain technology with IPFS and metadata-based attribution contributes to enhanced security and robustness of digital literary archives. This model provides a high level of tamper resistance and robust authorship validation, with minimal verification. The main advantage of the presented framework lies in its decentralized nature, which ensures transparency and immutability. Nevertheless, there are some limitations, including dependency on network scalability, transactional costs for blockchain, and increased computing power needs for larger implementations. Further development of this architecture can focus on optimization of lightweight consensus schemes and hybrid off-chain validation.

5 Conclusion

The framework Blockchain-Inspired Approach for Assurance of Texts' Authenticity and Attribution (BIAAF) has been presented in this research paper to resolve some of the core challenges facing the digital literary archives on authorship uncertainty, manipulation of textual contents, and provenance loss. The framework comprises a multilayered structure with a text ingestion layer, SHA-256-based cryptographic hashing, storing of smart contracts on the blockchain, decentralized document storing through IPFS technology, and a verification module for validation of integrity and authorship confirmation. The experiment results conducted using a dataset consisting of 50,000 documents of human-authored and artificially generated textual content have shown enhanced performance. The proposed approach has delivered the accuracy, precision, recall, and tampering detection rate of 99.2%, 96.8%, 95.4%, and 99.5%, respectively, along with keeping the verification time below 200 milliseconds. Compared to centralized and metadata-based archives, the model enhances security, reliability, and traceability. It also shows how efficient blockchain-powered decentralization could be in literary archiving. The significance of this model is in its ability to create immutable records of authorship and validate texts, particularly in the context of the growing influence of generative AI and the manipulation of digital content. Through the combination of blockchain immutability, decentralized

archiving, and metadata attributions, the model presents a robust tool for future digital literary archives infrastructure. There are some limitations to this study, which include the scalability of the blockchain, the cost of transactions, and computing power in large-scale usage. The future research will focus on the integration of AI-powered stylometric for authorship verification, the development of lightweight consensus mechanisms, and cross-chain compatibility for global digital literary archives.

References

[1] Adelia, N., Wahid, A., Alif, M., & Andaluzi, F. (2025). Digital Takhrij Hadith as Islamic Digital Humanities: Reconstructing Epistemic Authenticity and Transmission in the Digital Age. *Digital Muslim Review*, *3*(1), 83-96. https://doi.org/10.32678/dmr.v3i1.68

[2] Ailakhu, U. V. (2025). Blockchain for Long-Term Digital Archiving in Academic Libraries: Preserving Authenticity and Accessibility. *Access: An International Journal of Nepal Library Association*, *4*, 132-144. https://doi.org/10.3126/access.v4i1.88814

[3] Aldweesh, A. (2025). Blockchain-based secure firmware updates for electric vehicle charging stations in web of things environments. *World Electric Vehicle Journal*, *16*(4), 226. https://doi.org/10.3390/wevj16040226

[4] Alghathian, G. A., Krim, K. B. M., Khamaysa, M., & Altarawneh, M. (2026). Blockchain as a model for granting trust in AI-mediated digital transactions. *Frontiers in Blockchain*, *9*, 1770743. https://doi.org/10.3389/fbloc.2026.1770743

[5] AlKhanafseh, M., & Surakhi, O. (2024). Evidence preservation in digital forensics: An approach using blockchain and LSTM-based steganography. *Electronics*, *13*(18), 3729. https://doi.org/10.3390/electronics13183729

[6] Avelino, M., & Rocha, A. A. D. A. (2022). Blockproof: a framework for verifying authenticity and integrity of web content. *Sensors*, *22*(3), 1165. https://doi.org/10.3390/s22031165

[7] Awad, K. M., ElNainay, M., Abdeen, M., Torki, M., Saif, O., & Nabil, E. (2022). A secure blockchain framework for storing historical text: A case study of the holy Hadith. *Computers*, *11*(3), 42. https://doi.org/10.3390/computers11030042

[8] Demertzis, K., Rantos, K., Magafas, L., Skianis, C., & Iliadis, L. (2023). A secure and privacy-preserving blockchain-based XAI-justice system. *Information*, *14*(9), 477. https://doi.org/10.3390/info14090477

[9] Ejiyi, C. J., Obiora, S. C., Obiora, I., Wauk, G., Ejiako, M., Omotayo, T., & Bamisile, O. (2026). Impact of Generative AI on Author's Metrics and Copyright Ownership: Digital Labour, Ethical Attribution, and Traceability Frameworks for Future Internet Systems. *Future Internet*, *18*(4), 196. https://doi.org/10.3390/fi18040196

[10] Enayati, M., Arlikatti, S., & Ramesh, M. V. (2024). A qualitative analysis of rural fishermen: Potential for blockchain-enabled framework for livelihood sustainability. *Heliyon*, *10*(2). https://doi.org/10.1016/j.heliyon.2024.e24358

[11] Farhan, M., Butt, U., Sulaiman, R. B., & Alraja, M. (2025). Self-Sovereign Identities and Content Provenance: VeriTrust—A Blockchain-Based Framework for Fake News Detection. *Future Internet*, *17*(10), 448. https://doi.org/10.3390/fi17100448

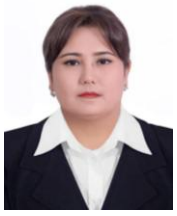
[12] Fitriawijaya, A., & Jeng, T. (2024). Integrating multimodal generative AI and blockchain for enhancing generative design in the early phase of architectural design process. *Buildings*, *14*(8), 2533. https://doi.org/10.3390/buildings14082533

[13] Han, P. (2025). AI-powered digital arbitration framework leveraging smart contracts and electronic evidence authentication. *Scientific Reports*, *15*(1), 37327. https://doi.org/10.1038/s41598-025-21313-x

[14] Khanzada, T. J., Shahid, M. F., Mutahhar, A., Aslam, M. A., Ashari, R. B., Jamal, S., ... & Siddiqui, S. (2023). Authenticity, and approval framework for bus transportation based on blockchain 2.0 technology. *Applied Sciences, 13*(20), 11323.

https://doi.org/10.3390/app132011323
[15] Khasanah, A. U., Kiman, R. O., & Prihandoko, D. (2025, December). Advancing Digital Sovereignty through Blockchain-Based Archival Systems: Global Insights and Indonesian Perspectives. In *2025 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)* (pp. 1556-1561). IEEE. https://doi.org/10.1109/ICIMCIS68501.2025.11327011
[16] Mohammed, A., Potdar, V., Quaddus, M., & Hui, W. (2023). Blockchain adoption in food supply chains: a systematic literature review on enablers, benefits, and barriers. *IEEE access*, *11*, 14236-14255. https://doi.org/10.1109/ACCESS.2023.3236666
[17] Omogiate, P. M., & Legal, C. A. T. (2022). Developing standardized metadata protocols enabling transparent provenance tracking for AI-created media within federal intellectual property regulatory systems nationwide. *International Journal of Computer Applications Technology and Research*, *11*(12), 711-723. https://doi.org/10.7753/IJCATR1112.1031
[18] Sonkamble, R. G., Phansalkar, S. P., Potdar, V. M., & Bongale, A. M. (2021). Survey of interoperability in electronic health records management and proposed blockchain based framework: MyBlockEHR. *IEEe Access*, *9*, 158367-158401. https://doi.org/10.1109/ACCESS.2021.3129284
[19] Vacchio, E. D., & Bifulco, F. (2022). Blockchain in cultural heritage: insights from literature review. *Sustainability*, *14*(4), 2324. https://doi.org/10.3390/su14042324
[20] Zhihui, F., Ruoyi, M., Shaowen, J., & Xiaofeng, G. (2026). A Credible Blockchain-Based Framework for Traceability in the Down-Product Supply Chain. *Applied Sciences*, *16*(11), 5456. https://doi.org/10.3390/app16115456

Authors Biography



Shakhnoza Khujamberdieva is a faculty member in the Department of Preschool Education at Namangan State Pedagogical Institute, Uzbekistan. Her research interests include digital education, information management, educational technologies, and contemporary approaches to knowledge preservation. She explores the impact of emerging technologies on academic and literary resources. Her scholarly work emphasizes data integrity, digital documentation, and innovation in educational systems. She actively contributes to interdisciplinary studies that connect technology and humanities. Her research supports the development of reliable frameworks for safeguarding digital content.

Mahliyo Khaydarova is an Associate Professor in the Department of Primary Education Methodology at Termez University of Economics and Service, Uzbekistan. Her academic interests include educational innovation, digital literacy, information security, and technology-enhanced learning environments. She investigates modern approaches to preserving and authenticating educational and literary resources. Her work focuses on integrating advanced digital solutions into knowledge management systems. She contributes to research addressing transparency and trust in digital information environments. Her studies promote innovative strategies for protecting intellectual and textual assets.

Gavhar Kurbanova is a researcher at Termez State Pedagogical Institute, Uzbekistan. Her research focuses on digital humanities, archival studies, educational technologies, and information authenticity. She is particularly interested in methods for preserving the integrity of literary and historical documents in digital formats. Her work examines the role of innovative computational systems in verifying authorship and content reliability. She has contributed to interdisciplinary projects involving technology and cultural heritage preservation. Her research supports sustainable digital archiving practices.

Navbaxor Shadiyeva is a Lecturer at Jizzakh State Pedagogical University, Uzbekistan. Her academic interests include language studies, digital documentation, information systems, and educational technologies. She explores technological approaches to ensuring transparency and accountability in digital archives. Her research examines frameworks for tracking authorship and preserving textual integrity in online repositories. She is actively involved in studies that combine humanities research with emerging digital tools. Her work contributes to advancing secure and trustworthy archival environments.

Gavhar Nurkulova is a teacher at Termez State University, Uzbekistan. Her research interests include digital communication, information management, educational technologies, and knowledge preservation. She investigates contemporary methods for securing digital records and maintaining content authenticity. Her work highlights the importance of transparent attribution systems in academic and literary archives. She has participated in research focused on technological solutions for safeguarding intellectual property. Her studies contribute to the development of reliable digital preservation frameworks.

Niginabonu Shokhimardonova is affiliated with Bukhara State Technical University and the National Research University "TIIAME," Uzbekistan. Her research focuses on information technologies, digital transformation, data security, and innovative archival systems. She is interested in the application of blockchain-inspired methodologies for ensuring authenticity and traceability in digital environments. Her scholarly work explores secure mechanisms for preserving textual ownership and provenance. She actively contributes to interdisciplinary research connecting technology and cultural heritage. Her studies support the advancement of trustworthy digital literary archives.

Shaxista Toxirjonova is a Senior Lecturer at Uzbekistan State World Languages University, Tashkent, Uzbekistan. Her academic interests include digital linguistics, corpus studies, information technologies, and literary documentation. She examines how emerging technologies can enhance the credibility and preservation of textual resources. Her research explores innovative approaches to authorship verification and content attribution in digital collections. She has contributed to studies on technology-assisted language and literary research. Her work promotes secure and transparent management of digital literary assets.

Barchinoy Isroilova is an Associate Professor in the Department of Primary Education at Andijan State Pedagogical Institute, Uzbekistan. Her research interests include educational innovation, digital knowledge systems, information ethics, and archival preservation. She investigates strategies for maintaining authenticity and accountability in digital academic resources. Her scholarly work focuses on integrating advanced technological frameworks into educational and literary repositories. She contributes to interdisciplinary research on digital trust and intellectual property protection. Her studies support the creation of sustainable and secure digital archive infrastructures.