International Journal of Computer Techniques–IJCT Volume 13 Issue 2, March-April - 2026

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

A Blockchain and IPFS Hybrid Architecture for Secure Storage and Distributed Verification of Academic Documents

Deepak Tomar
System Analyst, Computer Center
Bundelkhand University
Jhansi, India
dr.deepak@bujhansi.ac.in

Kismat Chhillar
Asst. Prof, Dept. of Mathematical Sciences & Computer Applications
Bundelkhand University
Jhansi, India
drkismatchhillar@gmail.com

***Abstract*—The rapid digitalization of management of academic record has amplified persistent concerns related to data breaches, document forgery and the shortcomings of centralized verification frameworks. Traditional databases of a university system relied on institutional trust and fragmented infrastructures, which limits cross-platform integration and leads to exposure of sensitive records to single failure points. This paper introduces a hybrid architecture integrating blockchain technology and the Inter Planetary File System (IPFS) for supporting secure storage and decentralized verification of academic documents. In the proposed model, academic records are first encrypted and then stored off-chain in IPFS. The cryptographic hashes and identifiers of content are recorded on the blockchain immutably through smart contracts, thus ensuring integrity, traceability and authenticity without incurring excessive storage costs for on-chain. The architecture ensures decentralized verification by permitting third-party stakeholders for validating documents through comparison of hash and contract-based proofs. This eliminates the need for validation processes that is manual or institution-specific. A comprehensive evaluation of security and performance demonstrated that the hybrid approach substantially improved scalability, reduced operational costs and enhanced privacy as compared to solutions that were completely centralized and blockchain-only. The findings indicated that blockchain and IPFS can be effectively integrated for establishing an interoperable, resilient and trust-reduced infrastructure for management of academic document in ecosystems of higher education.**

Keywords*— *Blockchain, IPFS, Academic Documents, Distributed Verification, Data Integrity, Smart Contracts

I. INTRODUCTION

Academic records such as degrees, transcripts and mark sheets serve as an important proof of educational achievement and are trusted by accrediting agencies, employers and academic institutions worldwide. Their integrity and authenticity are essential for credibility of an institution and success of an individual. However, as higher education progressively adopts digital platforms, these records needs to be safeguarded against tampering, enabling cross-border accessibility and ensuring verifiability have become major challenges. Most universities are still dependent on centralized databases which remain vulnerable to insider manipulation, data breaches and system failures. Such architectures also restricts interoperability and demands trust in custodianship of an institute. The growing complexity of tools for document forgery further complicates processes of verification, which often are dependant upon inconsistent standards and manual correspondence. Consequently, the academic field demands an urgent need for a transparent, secure and automated mechanism for management and verification of educational credentials. Blockchain does ensures transparency and immutability but storing complete academic documents directly on-chain becomes inefficient due to high costs, limited storage and barriers of scalability [1] [2]. As academic data is expanding at a fast pace across institutions, fully on-chain solutions have become impractical, making it essential to balance security advantages of blockchain with feasible strategies of storage. Current academic systems for verification also lack tamper-proof integrity and interoperability. Most of them are dependent on isolated institutional platforms without any universal standards, requiring trust in authorities that are centralized rather than assurance that is cryptographic [3]. The absence of verifiable and decentralized mechanisms continues to hinder efficient and cross-border validation of credentials [4].

In current study, a hybrid architecture is proposed that combines the Inter Planetary File System (IPFS) and blockchain to overcome the shortcomings of blockchain-only and centralized frameworks. It separates the storage of document from processes of verification, using IPFS for distributed, scalable storage and blockchain for verification of records and immutable metadata. The approach aims to ensures confidentiality, integrity and availability through hash-based tamper detection, document encryption and IPFS-driven redundancy. These mechanisms collectively works to safeguard the data against alteration, unauthorized access and system failure. Finally, the hybrid approach enables decentralized verification without any dependency on issuing institutions. On-chain hashes and Smart contracts allow third parties for validation of document authenticity independently. This in turn establishes a credentialing environment that is mathematically verifiable and trustless. This paper presents a hybrid model for storage and verification that integrates distributed storage that is off-chain with on-chain validation for efficient management of academic records. The framework considers issues of cost,

scalability and data integrity which in turn provides a practical foundation for deployment in ecosystems of higher education. Smart contracts govern access control, document registration and verification, ensuring automation, transparency and consistency across stakeholders. This mechanism reduces administrative overhead and increases accountability through auditable interactions. In academic scenarios, comprehensive evaluation illustrates the model's ability in enhancement of scalability, decrease of verification time and increase of security as compared to solutions that are centralized and blockchain-only.

The structure of remaining paper is as follows. Section 2 reviews related work highlighting existing gaps. Section 3 presents the proposed architecture, followed by Section 4, which details the process of document lifecycle and verification. Section 5 examines considerations of security and privacy, while Section 6 outlines the implementation of system, covers details about performance evaluation of the proposed system against baseline models and covers analysis of results. Sections 7 illustrates about discussion and comparative Analysis. Section 9 discusses about limitations and future directions. Section 10 finally concludes with key insights on secure and interoperable academic record management.

II. Background And Related Work

The growing digitization of academic records has highlighted limitations of centralized credential management systems, including risks of data tampering and single points of failure. Recent studies propose blockchain as a decentralized trust layer for issuing and verifying academic documents through immutable hash records and smart contracts. However, due to blockchain storage constraints, researchers increasingly advocate hybrid architectures that combine blockchain with IPFS, where documents are stored off chain and their hashes are anchored on chain for integrity and distributed verification.

A. Blockchain-Based Academic Record Systems

Research on credentialing that is blockchain-based has extensively explored Ethereum for issuance and verification of academic records by use of smart contracts that anchor on-chain credential hashes [5][6]. While Ethereum's integrity and non-repudiation, transparency and immutability support, reliance on external storage and excessive on-chain metadata reduce scalability, increase cost and raise concerns of privacy in large academic networks [7][8]. Consortium blockchains such as Quorum and Hyperledger Fabric address these shortcomings by restriction of participation to trusted institutions, improvement of efficiency and access control. However, their partial re-centralization of authority and governance complexity limit full decentralization, while processes of verification often remain institution-dependent.

B. IPFS for Distributed Storage

The Inter Planetary File System (IPFS) offers an approach to data storage that is decentralized and is based on content addressing, where identification of files is done by cryptographic hashes instead of location [9]. This mechanism supports deduplication, ensures integrity and enables distributed replication. This makes IPFS well suited for storing academic documents that are tamper-resistant with availability that is long-term [10] [11]. Prior studies have applied IPFS to areas such as medical, legal and management of intellectual property, demonstrating its durability and efficiency [12]. In the academic area, IPFS is frequently used as a supporting layer for systems that are traditional or blockchain-based [13][14].

C. Hybrid Blockchain-Off-Chain Architectures

Hybrid models of blockchain separate storage of data from verification logic, stores large files off-chain and records only essential metadata such as timestamps, hashes and ownership proofs on-chain. This structure minimizes transaction costs and storage while ensuring integrity and traceability of data, making it useful for management of digital assets [15][16]. Many existing frameworks use partially distributed or centralized systems that lack proper mechanisms of access control or revocation. While such models are effective in improving efficiency, few address comprehensive verification in academic contexts that is multi-stakeholder and thus limiting their practical adoption [17].

D. Research Gaps

Few studies thoroughly highlights distributed verification workflows that function without the need of issuing institutions. Verification is often treated as centralized or implicit rather than designed as a process that is decentralized governed by cryptographic proofs and smart contracts. This limits the realization of credential validation that is fully trustless and cross-institutional. Moreover, existing research rarely examines efficiency of scalability and cost under academic conditions that are realistic. Most works remain limited or conceptual to small prototypes, leaving long-term feasibility uncertain. This study addresses these research gaps through a holistic evaluation of framework encompassing transaction overhead, overall scalability, storage cost and verification latency.

III. System Architecture And Design

The proposed architecture integrates blockchain with IPFS to enable secure storage and decentralized verification of academic documents. Certificates are encrypted and stored on IPFS, which generates a unique content hash. This hash is recorded on the blockchain through a smart contract, ensuring immutability and transparent validation without storing the document on chain. By separating storage from verification, the design improves scalability, security and cost efficiency.

A. Architectural Overview

The proposed system introduces a hybrid architecture that integrates blockchain network and the Inter Planetary File System. This combines immutability of blockchain with distributed storage capability of IPFS. This approach maintains authenticity and traceability of document while avoiding the limitations of cost and scalability of storage that is full on-chain, offering a robust framework for large academic ecosystems. An important architectural principle is the separation of layers of storage and verification. Documents reside in IPFS, whereas metadata of hashes and verification are recorded on the blockchain. This structure preserves security through proofs that are immutable, reduces overhead that is on-chain and

allows each layer in evolving independently without affecting integrity of system.

B. Actors and Roles

Authorized bodies and universities serve as trusted issuers, encrypt academic documents, upload them to IPFS and record related metadata on the blockchain by using smart contracts. Issuance that is controlled or limited by verified institutions upholds authenticity and minimizes their role in subsequent verification. Ownership of the documents is held by the Students, with access that is bound to their digital identities. Permissioned access can be granted by them to verifiers without surrendering custody, thereby enhances privacy and individual control. Validation of documents by verifiers such as academic institutions or employers is done by retrieving them from IPFS and cross-checking proofs that are on-chain. This process of decentralization eliminates the need for mediation of an institution and thus ensures transparent and efficient validation. Figure 1 illustrates the hybrid architecture integrating blockchain network and IPFS.

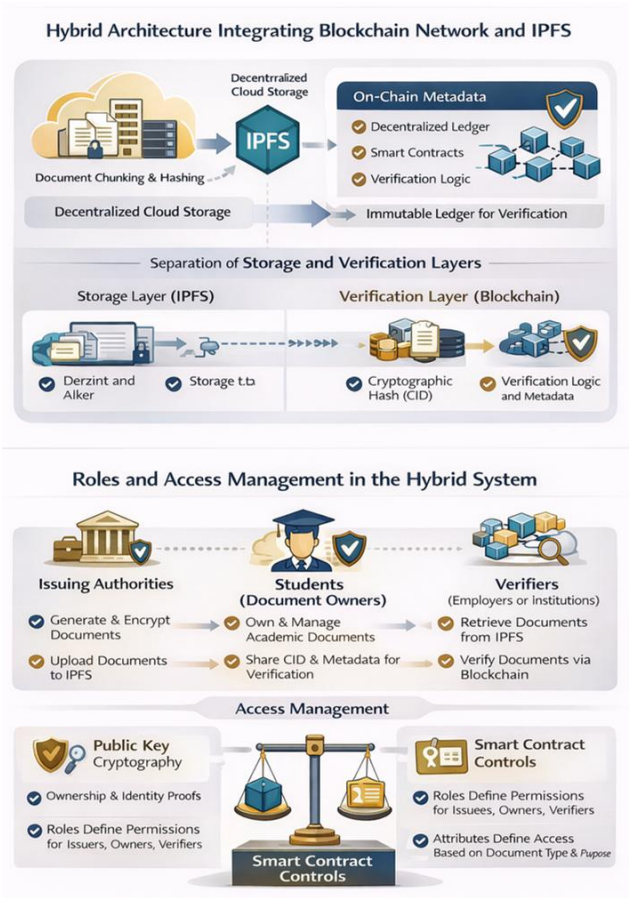

Fig 1: Hybrid Architecture integrating Blockchain Network and IPFS

C. IPFS-Based Document Storage

In the IPFS layer, academic documents are partitioned into smaller chunks and cryptographic hashes are assigned which ensures identification that is content-based rather than referencing that is location-based. Any alteration or tampering changes the hash which enables detection of instant tampering while improving efficiency and replication of storage across nodes. Before upload, encryption of documents is done for protecting sensitive information within the network that is distributed. Decryption keys are managed securely and shared only with authorized users. This maintain the confidentiality and transparency of verification that is blockchain-based.

D. Blockchain Layer

The blockchain keeps a record of essential metadata such as hashes, timestamps, IPFS content identifiers and ownership details in place of full documents. This approach minimizes costs of storage and transaction while maintaining verifiable integrity by the use of immutable on-chain references. Smart contracts provides management of document registration, verification and revocation, permitting only authorized institutions for issuing credentials. Automated execution ensures transparent and rule-based verification. This in turn creates a process that is auditable, trust-enhancing and free from manual intervention.

E. Access Control and Identity Management

The system utilizes public-key cryptography for authentication of participants and bind ownership of document to digital identities that are verified. Each user operates by using a cryptographic key pair which ensures secure identification, origin authenticity verification, and non-repudiation without exposure of personal data [18]. Access control combines mechanisms of role-based and attribute-based that are governed by smart contracts. Roles define permissions for owners, issuers and verifiers, while attributes provide specification of contextual constraints. This layered approach safeguards privacy, enforces institutional policies and ensures regulatory compliance.

IV. Document Lifecycle And Verification Workflow

The document lifecycle in the proposed hybrid framework begins with the generation of credential by the issuing authority, followed by encryption process and upload to IPFS, where a unique content hash is generated. This hash is then recorded on the blockchain through a smart contract for ensuring immutability and timestamped authenticity. During verification process, a stakeholder retrieves the document from IPFS and compares its generated hash with the hash stored on the blockchain. Any mismatch immediately indicates tampering, thereby enabling transparent, secure and decentralized validation throughout the lifecycle of the document.

A. Document Issuance Process

The lifecycle starts with the encryption of the academic document by the issuing institution prior to uploading it to the IPFS network. The encrypted file is then divided, distributed and replicated across nodes which results in ensuring confidentiality, availability and resistance to data loss. A content identifier that is unique and cryptographic hash are then generated and are recorded on the blockchain via smart contract, along with metadata of issuance and ownership [19].

This immutable record anchors the authenticity of the document and enables retrieval that is secure and verifiable. Figure 2 demonstrates the entire process of document lifecycle in the proposed hybrid framework.

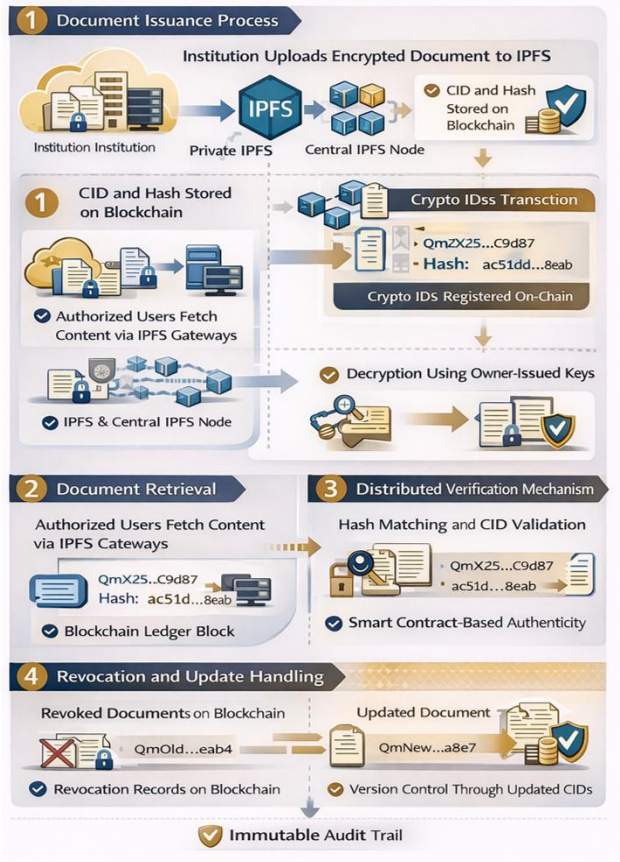

Fig 2: Document Lifecycle in Proposed Hybrid Framework

B. *Document Retrieval*

Encrypted documents are retrieved from the IPFS network by the authorized users using content identifiers recorded on the blockchain. Access occurs through gateways that are public or private and allows retrieval from any node that is hosting the content and ensures high availability without depending on a single source. Decryption is achieved using keys securely issued by the owner of the document and thus maintaining user control over access of data. This separation of rights of access from location of storage preserves autonomy and privacy while enabling retrieval that is efficient and decentralized.

C. *Distributed Verification Mechanism*

Verification involves recomputation of the cryptographic hash of the document and matching it with the hash that is stored on the blockchain. A valid match confirms integrity of the data and ensures conformity with the registered content identifier, allowing verification that is independent and without any institutional reliance. Smart contracts further perform automation of authenticity checks by verification of document registration and status of revocation on-chain. This transparent and rule-based mechanism produces consistent and auditable results that increases trust and prevent manipulation.

D. *Revocation and Update Handling*

When a document is found to be invalidated, the issuing institution records a revocation entry on the blockchain rather than deletion of prior data. A permanent audit trail is This preserved by this and marks the credential as revoked and also ensures the historical accountability and transparency. For corrections or updates, a new version that is encrypted is uploaded to IPFS, generating a unique content identifier linked to the original. This mechanism of versioning allows verifiers for distinguishing current documents from older ones, ensuring tamper-evident and traceable record management.

V. Security And Privacy Analysis

Tampering of a document poses a significant threat which involves attempts to alter academic records for malicious or illegal benefit. The model assumes attackers might access data that is stored or transmitted but cannot compromise blockchain consensus or cryptographic functions. Integrity is in turn preserved through mechanisms of verifiable hash-based validation. Risks of unauthorized access arise from both insider and external actors seeking decryption keys or confidential documents. The system tries to mitigate these threats through identity verification, encryption and controlled key sharing which ensures that only users those are authorized can access record contents. Traditional systems also face single points of failure from attacks or outages [20]. The model anticipates partial network failures and evaluates resilience through distributed storage and verification and thus ensures uninterrupted data availability.

Document integrity is ensured through cryptographic hashing and thus ensures any alteration producing a distinct hash. Storing of these hashes on the blockchain allows independent verification of authenticity without depending on centralized authorities. Immutability of blockchain that is supported by its consensus mechanism ensures that revocation entries and recorded metadata remain permanently auditable and tamper-evident which in turn reinforces long-term trust in records of an institution [21]. Availability is achieved through distributed design of IPFS, where replicated nodes preserve accessibility of document despite node failures or network disruptions, ensuring resilient and continuous and data retrieval. Academic documents are encrypted prior to being stored in the IPFS network, ensuring confidentiality within an environment that is publicly accessible. Encryption safeguards against unauthorized access while leveraging content-based retrieval and decentralized storage. To further protect privacy, only non-sensitive metadata such as content identifiers, hashes and verification states are stored on-chain [22]. Personal data remains off-chain and encrypted which in turn minimizes exposure and supports regulatory compliance without compromising of verifiability.

VI. Results And Performance Analysis

The system is deployed on a blockchain platform selected for balancing decentralization, performance and governance requirements. Public networks such as Ethereum support transparency in verification, whereas permissioned frameworks like Hyperledger Fabric offer controlled access that is suitable for consortium based academic environments. The IPFS layer operates through distributed nodes hosted on trusted institutional infrastructure for ensuring redundancy and fault tolerance. Smart contracts developed in Solidity manage the registration of credential by recording document hashes, content identifiers, ownership metadata and timestamps on the blockchain. Mechanisms of Access control restrict issuance to authorized entities, while verification and revocation functions maintain integrity and auditability. A prototype implementation integrates blockchain and IPFS nodes with dedicated interfaces for issuers, holders and verifiers, deployed in a controlled and containerized environment for evaluation of reliability, scalability and security under realistic academic conditions.

The performance evaluation utilizes a representative dataset of academic records including degree certificates, transcripts and mark sheets of diverse formats and sizes to reflect real-world institutional workloads. This dataset incorporates both structured text documents and larger scanned files, enabling precise measurement of storage efficiency, retrieval latency and verification speed under realistic conditions. The experimental framework models a distributed environment with blockchain and IPFS nodes deployed across multiple logical sites, where network scale and node distribution are systematically varied. Through this setup, the study examines how decentralization influences throughput, scalability and availability, providing robust insights into the operational performance of the system across heterogeneous academic contexts. The performance evaluation assesses latency, storage efficiency, throughput and scalability for determining the effectiveness of the proposed hybrid architecture. Storage costs are compared with fully on chain models by examining of blockchain transaction fees and data requirements alongside IPFS overhead, revealing substantial cost reductions through off chain storage while preserving verifiability and integrity. Upload latency measures the time that is required for encryption, storage and registration of blockchain, whereas verification latency captures the processes of retrieval and hash validation. Scalability and throughput are analyzed under increasing volume of documents and concurrent verification requests, demonstrating stable performance and clear advantages over fully on chain approaches in terms of cost efficiency and operational responsiveness.

A. Comparison with Fully On-Chain Approaches

The results indicate that the proposed hybrid architecture significantly outperforms fully on-chain solutions in terms of storage efficiency and transaction cost. Fully on-chain approaches incur substantial overhead when storing large documents, leading to higher costs and reduced throughput. In contrast, the hybrid model confines blockchain usage to lightweight metadata, enabling faster transactions and improved scalability while preserving strong security guarantees. Figure 3 illustrates the storage cost comparison between architectures.

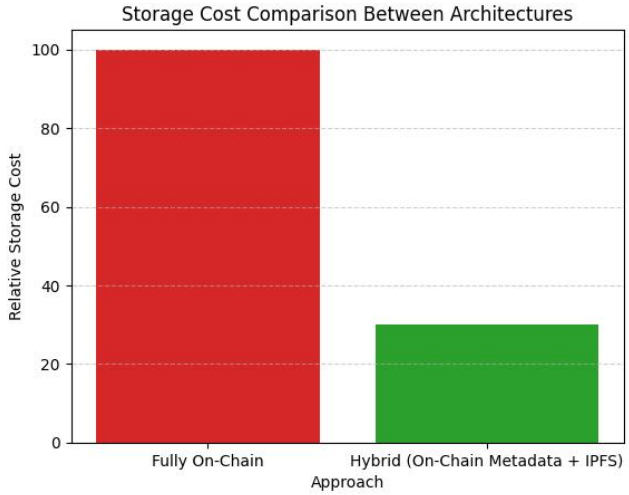

Fig 3: Storage Cost Comparison Between Architectures

Fully on-chain storage leads to excessive blockchain growth, increasing storage costs and limiting scalability. The hybrid architecture significantly reduces storage overhead by offloading large documents to IPFS. Figure 4 shows the transaction cost comparison between architectures.

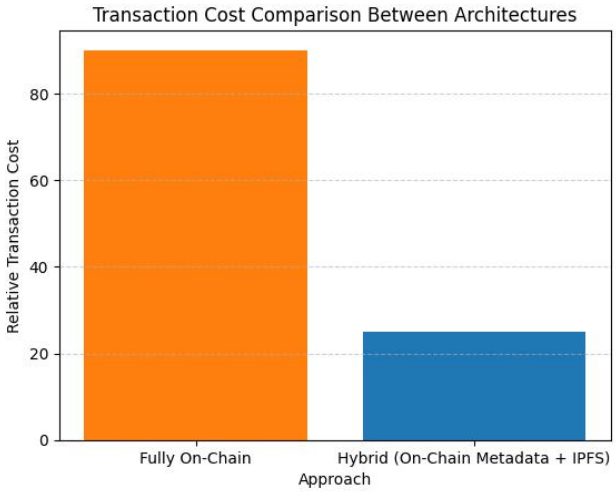

Fig 4: Transaction Cost Comparison Between Architectures

B. Impact of Document Size on Performance

Analysis of document size reveals that larger documents have minimal impact on blockchain performance due to off-chain storage in IPFS. While upload time increases proportionally with document size during the IPFS storage phase, verification latency remains largely unaffected, as it

relies on fixed-size hash comparisons. This result highlights the suitability of the proposed architecture for managing diverse academic documents without compromising verification efficiency. Figure 5 and figure 6 shows the effect of document size on IPFS upload time and blockchain verification latency respectively.

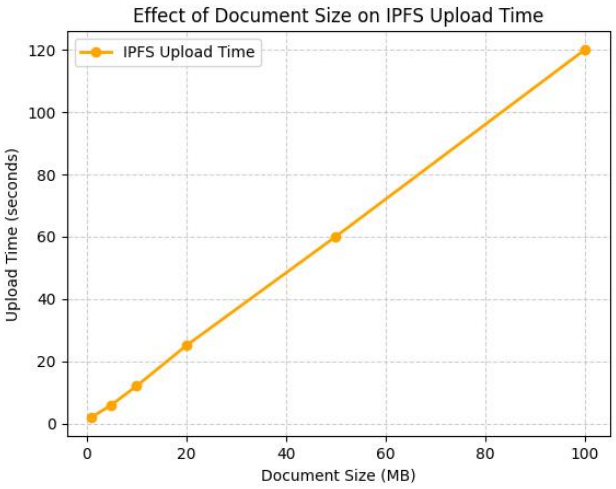

Fig 5: Effect of Document Size on IPFS Upload Time

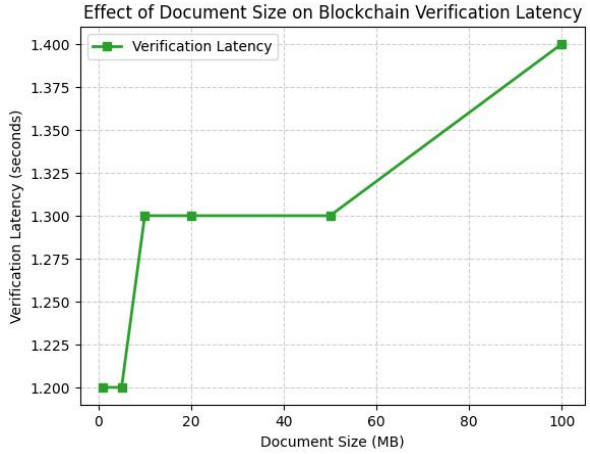

Fig 6: Effect of Document Size on Blockchain Verification Latency

Traditional on-chain systems experience significant overhead when handling large documents, resulting in higher expenses and reduced throughput. By limiting blockchain interactions to lightweight metadata, the hybrid approach achieves faster transactions, improved scalability and uncompromised security. Further analysis shows that document size has minimal effect on performance, as large files are stored off-chain in IPFS. Although upload time increases with document size, verification latency remains stable because it depends only on fixed-size hash comparisons. These results confirm the architecture's suitability for managing a wide range of academic documents without sacrificing verification speed or system performance. Table 1 illustrates the impact of document size on IPFS upload time and verification latency.

TABLE I. IMPACT OF DOCUMENT SIZE ON IPFS UPLOAD TIME AND VERIFICATION LATENCY

Document Size (MB)	IPFS Upload Time (s)	Blockchain Verification Latency (s)
1	2	1.2
5	6	1.2
10	12	1.3
20	25	1.3
50	60	1.3
100	120	1.4

C. Comparison with Centralized Systems

Centralized academic document management systems rely on institution-controlled databases that require verifiers to trust issuing authorities and often involve manual or semi-automated verification processes. While these systems are relatively simple to deploy, they are vulnerable to single points of failure, data breaches and administrative delays. In contrast, the proposed hybrid blockchain and IPFS architecture decentralizes trust by anchoring verification in cryptographic proofs rather than institutional assurances. This shift reduces verification latency, enhances resilience against system outages and improves transparency, particularly in cross-institutional and international verification scenarios. Figure 7 demonstrates the comparison of centralized and hybrid blockchain-IPFS systems.

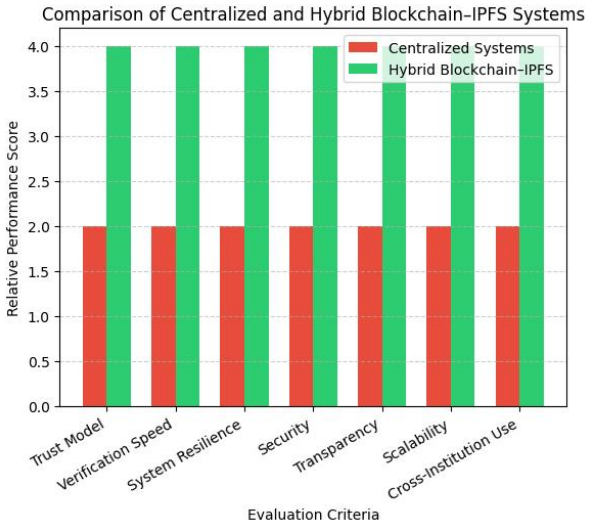

Fig 7: Comparison of Centralized and Hybrid Blockchain-IPFS Systems

D. Comparison with Blockchain-Only Solutions

Blockchain-only approaches attempt to leverage immutability and transparency by storing academic records directly on-chain or by maintaining extensive on-chain metadata. Figure 8 shows the comparison of proposed hybrid system with blockchain-only systems.

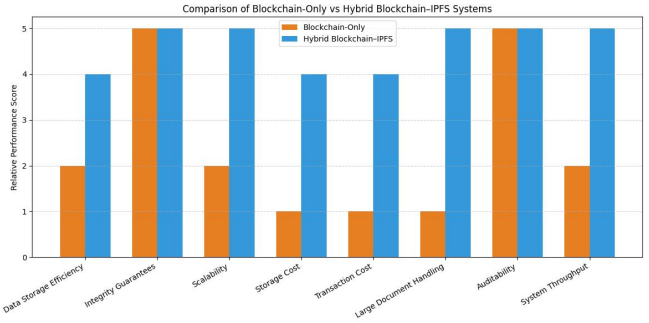

Fig 8: Comparison of Blockchain-Only and Hybrid Blockchain-IPFS Systems

Although such systems provide strong integrity guarantees, they suffer from scalability limitations, high storage costs and inefficient handling of large documents. The hybrid architecture addresses these limitations by offloading document storage to IPFS while retaining blockchain-based verification. This separation significantly reduces on-chain data overhead and transaction costs, enabling the system to scale more effectively without compromising security or auditability.

E. Cost, Scalability, and Trust Trade-Offs

The comparative evaluation highlights important trade-offs among cost, scalability and trust across different system designs. Centralized systems offer low initial deployment costs but incur long-term operational inefficiencies and trust dependencies. Figure 9 summarizes the comparison of cost, scalability and trust across system designs.

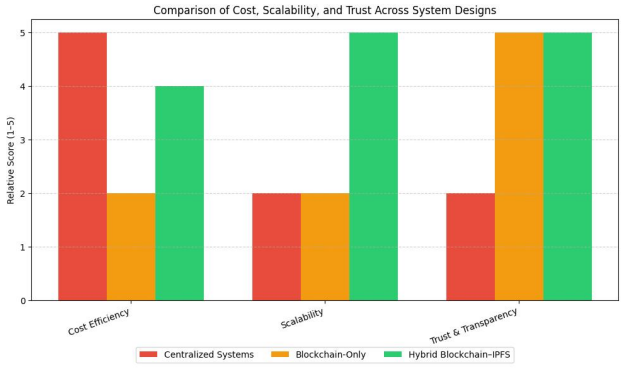

Fig 9: Comparison of Cost, Scalability and Trust across System Designs

Blockchain-only solutions enhance trust and transparency but introduce prohibitive costs and scalability constraints. The proposed hybrid model achieves a balanced trade-off by minimizing on-chain costs, supporting large-scale document storage and maintaining decentralized trust through immutable verification records. This balance makes the hybrid approach particularly well suited for sustainable and interoperable academic document management.

VII. Limitations And Future Scope

While IPFS enhances data resilience through distributed storage, document availability still depends on active nodes and effective strategies of pinning. Insufficient redundancy or node downtime can reduce the performance of retrieval, underscoring the importance of institutional pinning policies and continuous monitoring. In parallel, successful large-scale adoption of the proposed architecture requires well-defined frameworks of governance, especially within consortium blockchain involving multiple institutions. Establishing participation rules, trust models and policy coordination can be complex, suggesting the need for automated governance and onboarding mechanisms that maintain decentralization while minimizing administrative burden.

The current implementation assumes cryptographic identities managed at the application level, which may limit interoperability with broader digital identity ecosystems. Integrating decentralized identity standards such as verifiable credentials and decentralized identifiers could enhance user control, portability and privacy. Future work will focus on aligning the proposed architecture with emerging identity standards to enable seamless integration with external identity providers, support selective disclosure and further strengthen trust-minimized verification across academic and professional domains.

VIII. Conclusion

This study presents a hybrid architecture that integrates blockchain and IPFS in enhancing academic document management through secure storage, decentralized verification and automated access control. The system leverages off-chain storage with on-chain verification for reducing cost and improve scalability while maintaining integrity and auditability. Experimental results confirmed that restricting blockchain usage to metadata significantly lowers overhead and transaction expenses without compromising security. By enabling trust-minimized and institution-independent verification, the framework strengthens transparency, prevents credential fraud and empowers students with secure ownership and verifiable control of their records, supporting the evolution of resilient and decentralized academic ecosystems.

References

[1] H. Eren, Ö. Karaduman and M. T. Gençoğlu, "Security Challenges and Performance Trade-Offs in On-Chain and Off-Chain Blockchain Storage: A Comprehensive Review," *Applied Sciences*, vol. 15, no. 6, p. 3225, 2025.

[2] I. S. Rao, M. L. M. Kiah, M. M. Hameed and Z. A. Memon, "Scalability of blockchain: a comprehensive review and future research direction," *Cluster Computing*, vol. 27, no. 5, pp. 5547-5570, 2024.

[3] M. Al Hemairy, M. Abu Talib, A. Khalil, A. Zulfiqar and T. Mohamed, "Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation:

UAE case study and system performance (2022)," *Education and Information Technologies*, vol. 29, no. 14, pp. 18203-18232, 2024.

[4] C. Udokwu, P. Brandtner, A. Norta, A. Kormiltsyn and R. Matulevičius, "Implementation and evaluation of the DAOM framework and support tool for designing blockchain decentralized applications," *International Journal of Information Technology*, vol. 13, no. 6, pp. 2245-2263, December 2021.

[5] N. Nadeem, M. F. Hayat, M. A. Qureshi, M. Majid, M. Nadeem, and J. Janjua, "Hybrid Blockchain-based Academic Credential Verification System (B-ACVS)," *Multimedia Tools and Applications* 2023 82:28, vol. 82, no. 28, pp. 43991–44019, Apr. 2023, doi: 10.1007/S11042-023-14944-7.

[6] C. A. Hossain, M. A. Mohamed, M. S. R. Zishan, R. Ahasan and S. M. Sharun, "Enhancing the security of E-Health services in Bangladesh using blockchain technology," *International Journal of Information Technology*, vol. 14, no. 3, pp. 1179-1185, May 2022.

[7] H. F. Atlam *et al.*, "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions," *Electronics 2024, Vol. 13,* vol. 13, no. 17, Sep. 2024, doi: 10.3390/ELECTRONICS13173568.

[8] M. Boughdiri, T. Abdellatif, and C. Ghedira Guegan, "A Systematic Literature Review on Blockchain Storage Scalability," *IEEE Access*, vol. 13, pp. 102194–102219, 2025, doi: 10.1109/ACCESS.2025.3578451.

[9] A. Kumar and V. P. Kumar, "An Approach to Secure Decentralized Storage System Using Blockchain and Interplanetary File System," *2023 IEEE International Conference on Blockchain and Distributed Systems Security, ICBDS 2023*, 2023, doi: 10.1109/ICBDS58040.2023.10346339.

[10] P. K. Laboso, A. Martin, and P. Thiyagarajan, "A Secure System for Decentralized Preservation of Digital Library Collections Using Private Blockchain and Interplanetary File System (IPFS)," *Communications in Computer and Information Science*, vol. 2232 CCIS, pp. 331–341, 2025, doi: 10.1007/978-3-031-75608-5_26.

[11] M. R. Haque, S. I. Munna, S. Ahmed, M. T. Islam, M. M. H. Onik, and A. B. M. A. Rahman, "An Integrated Blockchain and IPFS Solution for Secure and Efficient Source Code Repository Hosting using Middleman Approach," *PLoS One*, vol. 20, no. 9 September, Sep. 2024, doi: 10.1371/journal.pone.0331131.

[12] K. Tiwari and S. Kumar, "A healthcare data management system: blockchain-enabled IPFS providing algorithmic solutions for increased privacy-preserving scalability and interoperability," *The Journal of Supercomputing 2025,* vol. 81, no. 8, pp. 895, May 2025, doi: 10.1007/S11227-025-07400-W.

[13] I. C. A. Pilares *et al.*, "Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS," *Sensors 2022,* vol. 22, no. 11, May 2022, doi: 10.3390/S22114032.

[14] R. K. Mishra, R. K. Yadav, and P. Nath, "Integration of Blockchain and IPFS: healthcare data management & sharing for IoT Environment," *Multimedia Tools and Applications 2024 84:23*, vol. 84, no. 23, pp. 27229–27250, Sep. 2024, doi: 10.1007/S11042-024-20092-3.

[15] A. K. Mishra and Y. Mohapatra, "Hybrid blockchain based medical data sharing with the optimized CP-ABE for e-Health systems," *International Journal of Information Technology*, vol. 16, no. 1, pp. 121-130, January 2024.

[16] G. Han, Y. Ma, Z. Zhang, and Y. Wang, "A hybrid blockchain-based solution for secure sharing of electronic medical record data," *PeerJ Comput Sci*, vol. 11, p. e2653, Jan. 2025, doi: 10.7717/PEERJ-CS.2653/SUPP-10.

[17] T. Temitope, "Investigating Innovative Models of Governance and Collaboration for Effective Public Administration in a Multi-Stakeholder Landscape," *International Journal Papier Public Review*, vol. 4, no. 2, pp. 18–28, May 2023, doi: 10.47667/IJPPR.V4I2.209.

[18] A. Srivastava and J. Gupta, "Attack resistant blockchain-based healthcare record system using modified RSA Algorithm," *International Journal of Information Technology*, vol. 16, no. 1, pp. 417-424, January 2024.

[19] N. C. Gowda and A. Bharathi Malakreddy, "BPCPR-FC: blockchain-based privacy preservation with confidentiality using proxy reencryption and ring signature in fog computing environments," International Journal of Information Technology, vol. 15, no. 6, pp. 3343-3357, August 2023

[20] R. Chaganti, R. V. Boppana, V. Ravi, K. Munir, M. Almutairi and F. Rustam, "A Comprehensive Review of Denial of Service Attacks in Blockchain Ecosystem and Open Challenges," *IEEE Access*, vol. 10, pp. 96538-96555, September 2022.

[21] P. Maheshwari and S. Gupta, "Integrating Self-Signed Key Cryptography with Blockchain for Decentralized Digital Record Authentication," in *2025 6th International Conference on Communication, Computing & Industry 6.0 (C2I6)*, Bangaluru, India, 2025.

[22] X. Tao, Y. Liu, P. K.-Y. Wong, K. Chen, M. Das and J. C. Cheng, "Confidentiality-minded framework for blockchain-based BIM design collaboration," *Automation in Construction*, vol. 136, p. 104172, April 2022.