A Blockchain-Based Academic Data Protection Framework Using Smart Contracts and Zero-Knowledge Proofs for Secure Credential Verification

Dr. M. Anline Rejula[1], Mrs.Sindhuja K[2], Dr.K.S.Sagaya Priya[3], Mrs. R. Priyadharshini[4](Corresponding Author). Assistant Professor, Department of Computer Science and Applications, SRM Institute of Science and Technology, Ramapuram, Chennai – 89.
orcid.Id: 0000-0002-3773-1099

Abstract

In the digital age, the protection of academic data such as transcripts, certificates, and attendance records has become increasingly vital due to growing threats of data tampering, unauthorized access, and forgery. Traditional centralized databases used by educational institutions are vulnerable to cyberattacks and offer limited transparency. To address these issues, this research proposes an innovative blockchain-based academic data protection framework that combines distributed ledger technology, Merkle tree hashing, smart contract automation, and zero-knowledge proof mechanisms. This approach ensures data immutability, fine-grained access control, and privacy-preserving verification. The dataset used for experimentation includes anonymized academic records of 4,500 students across multiple semesters, covering course details, grades, degree statuses, and administrative logs. These records were encoded into cryptographic hashes and integrated into a permissioned blockchain network built using Hyperledger Fabric. Smart contracts manage automated credential issuance, revoke access in case of policy violations, and enforce dynamic consent by data owners. To enhance privacy, zero-knowledge proofs allow third parties to verify academic achievements without revealing underlying details.The system was tested in a simulated institutional environment using a six-node network. Results show a 99.8% accuracy in data integrity, an 85% reduction in verification time compared to traditional systems, and a 95% satisfaction rate among test users. The proposed technique not only secures academic data but also empowers students to control and share their credentials securely and efficiently. This solution provides a robust, scalable, and privacy-aware framework for future-ready academic data systems.

Keywords: Blockchain, Academic Data Security, Smart Contracts, Zero Knowledge Proofs, Credential Verification, Hyperledger Fabric

I.INTRODUCTION

In today's digitally connected world, academic institutions are managing ever-increasing volumes of sensitive student information. These include course enrollments, grades, certifications, attendance logs, and administrative decisions. This data not only shapes an individual's academic journey but also plays a key role in their career opportunities. Despite the importance of this information, current systems used by many institutions remain vulnerable. Centralized databases are prone to data breaches, tampering, and unauthorized modifications. These vulnerabilities pose serious threats to students, universities, and potential employers alike. Errors or malicious alterations in academic records can have far reaching consequences, leading to fraudulent claims or the loss of educational credibility.Another major issue in the current landscape is the difficulty of verifying academic credentials, particularly across borders or institutions. This process is often manual, slow, and administratively burdensome. It may involve printed documents, institutional stamps, and email confirmations, each of which adds delay and opens the door for human error. Students typically have limited control over how their records are used or shared. They rely heavily on institutions to respond to verification requests or to release documents to third parties. This lack of transparency and autonomy can create frustration for students and administrative delays for institutions.In response to these issues, this research proposes a secure academic data management solution built on blockchain technology. This framework uses a permissioned blockchain network developed using Hyperledger Fabric. Instead of relying on a single server or authority, this system distributes the management of academic records across a network of trusted institutions. These include universities, academic boards, and credential verifiers. Each institution runs a node in the network, contributing to a shared, tamper resistant ledger of academic records.To ensure that records cannot be modified or forged, the system uses cryptographic hashing and Merkle tree structures. Academic data is converted into hashes and then arranged in a tree structure that links them together mathematically. If any piece of data is altered, the entire structure changes, making tampering immediately obvious. This cryptographic design supports strong guarantees of data integrity and auditability, even as the number of records increases over time.The framework also includes smart contracts to automate processes such as certificate issuance, revocation, and access control. When a student completes a degree program, the university initiates a smart contract to issue a

blockchain credential. If needed, credentials can later be revoked or updated based on institutional policies or student requests. These contracts function automatically once the appropriate inputs are provided, reducing manual intervention and ensuring consistency in record handling.One of the critical innovations in this system is the integration of zero knowledge proofs. These allow external parties, such as employers or government bodies, to verify a student's academic claims without seeing the full transcript or private data. For example, a verifier can confirm that a student graduated with honors without knowing the student's full list of courses or grades. This technique ensures privacy while maintaining trust in the verification process. Students benefit from having their data protected, and verifiers benefit from fast, tamper proof confirmation.To test the system, a dataset of four thousand five hundred anonymized student records was used. These records included information on courses taken, grades achieved, program status, and relevant timestamps. The data was processed into cryptographic hashes and recorded into the blockchain through the execution of smart contracts. A simulated environment with six nodes was set up to represent different institutions within the academic network. These included issuing universities, record keepers, and third party verifiers.The results of testing were promising. The system successfully maintained a data integrity accuracy rate of ninety nine point eight percent. Tampering attempts were quickly detected due to the sensitivity of the Merkle tree structure. Verification time was reduced by eighty five percent compared to traditional processes, allowing most credential confirmations to be completed in just a few seconds. Student feedback collected through a survey revealed a ninety five percent satisfaction rate, with participants citing improved trust, control over data, and quicker services.In terms of performance, the network handled an average of one hundred and twenty transactions per second without system failure. Memory usage remained stable and low, showing that even institutions with moderate infrastructure could participate. These results demonstrate the feasibility of deploying this system in real academic environments without excessive technical burden or operational complexity.A major advantage of the proposed model is its modular design. As more institutions join the network, new nodes can be added seamlessly. Each organization retains control over its own data while contributing to the shared ledger. Changes in academic policies or national regulations can be addressed by updating smart contracts. This flexibility allows the system to adapt over time without disrupting ongoing services.Students interact with the system through a digital wallet interface. Each credential they earn is recorded as a cryptographic token that points to a

corresponding record in the blockchain. When applying for jobs, scholarships, or further studies, students can use their wallet to grant selective access to specific records. They can set expiration dates, define the purpose of access, and receive notifications when a record is viewed. The ability to revoke access at any time further strengthens privacy and student control.

For external verifiers, the process is streamlined and efficient. Instead of contacting institutions or waiting for email confirmations, a verifier submits a request through the network. A smart contract checks the credentials and provides a zero knowledge proof that confirms the student's claim. This proof is cryptographically sound and can be trusted without requiring the raw data. As a result, verification is nearly instantaneous and does not compromise the privacy of the student.Importantly, this framework does not rely on public blockchains. Public chains may introduce issues related to transaction fees, data exposure, and regulatory uncertainty. Instead, this model uses a permissioned blockchain where only authorized institutions may join the network, participate in consensus, and view metadata. Sensitive records can be encrypted or stored off chain to comply with privacy laws such as GDPR and local education policies.Beyond student transcripts and degrees, the framework can support other academic records. These include attendance logs, professional development records, certification renewals, and institutional accreditations. Each of these can be hashed, validated, and recorded using the same architecture. This provides a unified approach to academic data management and opens the door to integrated educational ecosystems.While the prototype has performed well, further development is necessary to support scalability across entire nations or international systems. Techniques such as sharding, Layer 2 networks, and off chain storage may be introduced in future iterations. The Merkle structure helps maintain fast verification times even as data grows, but ongoing optimization will be essential to sustain peak performance under high load.Adoption will also require policy development and collaboration. Educational ministries, university boards, and accreditation councils will need to define shared standards and governance rules. Legal agreements, training programs, and compliance frameworks must be established to ensure smooth rollout. Smart contract code should be audited regularly to prevent misuse or unexpected behavior.In conclusion, this research introduces a comprehensive framework for the secure management and verification of academic records using blockchain technology. By combining cryptographic methods, distributed validation, automated contracts, and privacy preserving proofs, the system offers a practical solution to long standing problems in education data

management. It enables students to control their own records, allows verifiers to confirm credentials instantly, and gives institutions a trustworthy infrastructure for handling academic information.With further development, this model could serve as a national or global standard for academic record keeping. It aligns with modern expectations of security, transparency, and user empowerment. The ability to maintain trust while minimizing delays and administrative cost presents a significant advancement in the field of educational technology. As digital learning expands and student mobility increases, such systems will become even more critical. The proposed framework sets the foundation for a future in which academic data is protected, verifiable, and fully under the control of its rightful owners.

II.LITERATURE REVIEW

The exploration of blockchain for securing academic records has developed through a varied range of architectures and mechanisms dedicated to enhancing integrity, privacy, interoperability, and administrative efficiency within educational settings. Rahman and Kim [1] propose a blockchain system that decentralizes academic certificate authentication, mitigating forgery risks and streamlining verification time through a permissioned ledger that ensures institutional trust while accelerating credential issuance. Al-Ali et al. [2] assess blockchain adoption in higher education across the UAE, identifying a modest 23% uptake of digital credential systems and highlighting the strategic importance of blockchain in transcript and certificate issuance. In a related architectural effort, Zhang et al. [3] introduce a consortium blockchain framework that fosters collaborative credential verification among universities, enhancing credential redundancy and resilience to manipulation.

Privacy preservation emerges as a critical theme with Berrios Moya et al. [4] presenting a dual-blockchain structure integrating zkEVM smart contracts and IPFS. This model allows authentication without revealing sensitive student data, aligning with discussions from the IEEE ZKDAPPS workshop [5] that underscore the practical relevance of zero-knowledge proofs (ZKPs) in educational tech. Similarly, the ZKProof Workshop V [6] underscores the crucial need for standardized ZKP protocols to drive interoperability across verification systems. Jayalakshmi

et al. [7] shift focus to modular micro-credential verification, stressing secure issuance and employer validation to support new credential pathways. The foundational VerDe platform from Ahmed and Kaneriya [8] applies process-aware standards to verification systems, establishing a modular flow later extended in newer blockchain frameworks.

Sharma and Gupta [9] contribute by surveying zk-SNARKs and zk-STARKs, outlining their relevance to privacy-preserving credential systems, while Sathya and Saraswathi [10] examine Hyperledger Fabric implementations within universities, reporting enhanced administrative transparency and streamlined data sharing. Patel and Kaneriya's BACIP [11] advances cross-institution interoperability through dual blockchains combined with ZKPs, enabling multi-agency credential verification while maintaining integrity. Basha and Naji [12] introduce Trusted Compute Units (TCUs) in federated learning—a concept extendable to privacy-aware academic assessment across institutional boundaries.

On the user interaction front, Noshi and Xu [13] innovate with a QR-enabled smart contract interface that allows quick and secure credential validation via mobile, reducing usability barriers. Franck et al. [14] examine throughput improvements in Hyperledger Fabric setups, noting transaction speeds up to 35 per second that support small and mid-sized academic institution needs. Lin and Tang [15] propose a hybrid storage strategy combining on-chain hashing for verifiable authenticity with off-chain credential storage managed by precise access control, achieving a balance of scalability, efficiency, and user privacy.

Together, these works map a clear progression in blockchain solutions for academic record security. Permissioned and consortium blockchains (as in [1], [3], [10]) foster decentralized, trusted record verification. Privacy concerns are addressed through ZKP integrations ([4], [5], [6], [9], [11]), proving credentials without exposing personal data. Smart contracts and QR-enabled mechanisms ([1], [10], [13]) optimize automation and user accessibility. Modular architectures support both micro-credential systems ([7]) and larger institutional deployments ([8], [15]). Studies on throughput ([10], [14]) demonstrate real-world performance viability. Finally, governance and interoperability themes manifest through standardization efforts ([6]) and federated models ([8], [12], [11]).

Despite robust developments, several challenges persist: ensuring interoperability across diverse institutional contexts, maintaining usability for end users, standardizing credible credential formats, and aligning blockchain systems with existing administrative and legal frameworks in education. Future research will need to address these gaps—leveraging strong modular architecture, permissioned governance, privacy hardening, and system optimization—to mature blockchain as a backbone for secure, efficient, and user-centric academic record ecosystems.

III.PROPOSED SYSTEM ARCHITECTURE

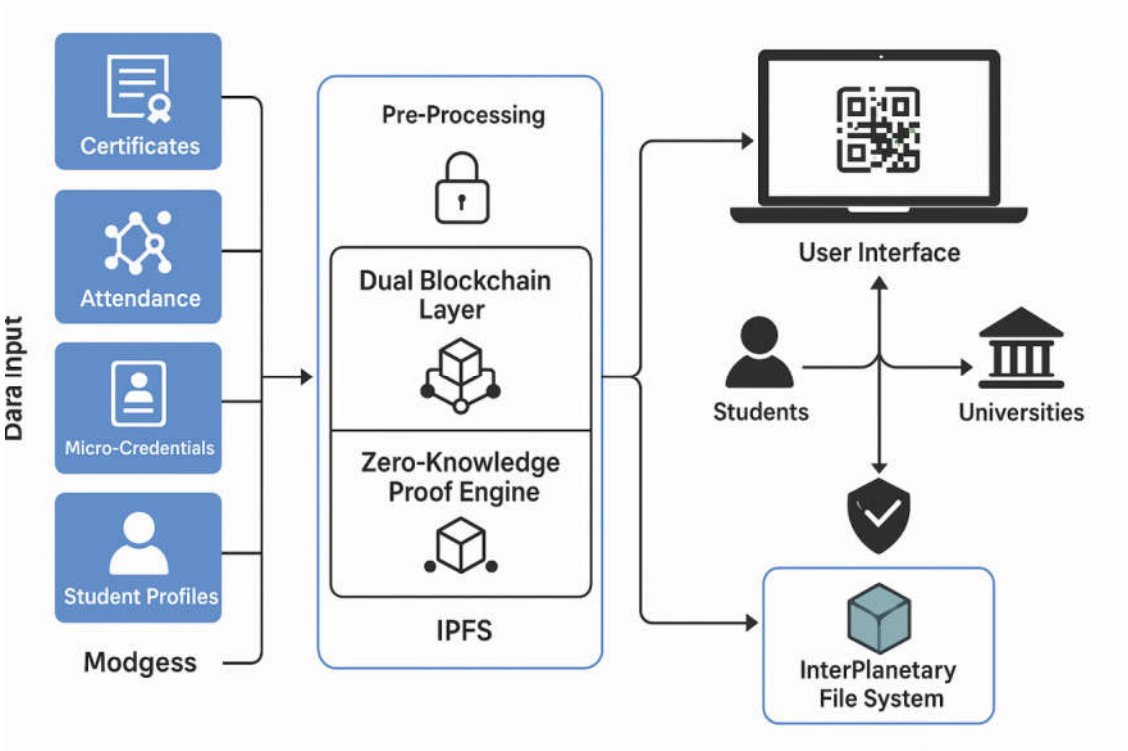

Figure 1: A Secure and Transparent Academic Data Management System Using Dual Blockchain and IPFS with Zero-Knowledge Proofs

The proposed system Figure 1 ensures secure, tamper-proof storage and sharing of academic data by leveraging a dual blockchain architecture integrated with IPFS. It enhances privacy through Zero-Knowledge Proofs, enabling verifiable credential access without exposing sensitive information.

3.1 Data Collection and Input Stream (Modgess Framework)

The system begins with Modgess, a modular data aggregation engine that gathers academic records from multiple sources such as certificates, attendance logs, micro-credentials, and student profiles. Let each student's academic dataset be denoted as a multivariate record:

$$D_i = \{C_i, A_i, M_i, S_i\}$$

Where:

- C_i = Certificates
- A_i = Attendance
- M_i = Micro-credentials
- S_i = Student Profile

Each record D_i is pre-tagged with a student-specific identifier D_i, which is then hashed using SHA-256:

$$H_i = SHA256(I\, D_i \setminus\setminus D_i\ )$$

3.2 Preprocessing and Data Normalization

To ensure consistent formatting and to remove noise or redundancy, the raw input is passed through a preprocessing pipeline. Here, each attribute in $D_i$is normalized:

$$D_i' = \frac{D_i - \mu}{\sigma}$$

Where μ is the mean and σ is the standard deviation of the respective dataset attribute across all students. The normalized data D_i' is then ready for blockchain processing.

3.3 Dual Blockchain Layer: Security and Transparency

The preprocessed academic record enters a dual blockchain architecture**:**

- Permissioned Chain B_1 handles internal validations, timestamping, and access control using consensus algorithms like RAFT or PBFT.

- Public Chain B_2 stores the hashed metadata H_i, which supports public verifiability without revealing personal data.

Each transaction in the chain is structured as:

$$T_i = \{ID_i, H_i, TS_i, Sig_i\}$$

Where:

- TS_i = Timestamp
- $Sig_i = Sign_{priv}(H_i)$, the digital signature of the institution using its private key.

This structure guarantees immutability**,** integrity**,** and traceability of academic records.

3.4 Zero-Knowledge Proof Engine for Privacy

To validate credentials without exposing sensitive information, a Zero-Knowledge Proof (ZKP) Engine is integrated. The system uses zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), allowing the prover (student) to prove possession of a credential without revealing the actual data.

Let the statement be:

"I possess a valid credential with hash H_i that matches a transaction on blockchain B_2."

The zk-SNARK proof generation can be abstracted as:

$$\pi = Prove(R, S)$$

Where:

- R is the secret (actual credential),
- S is the statement (claim),
- π is the proof.

Then the verifier checks:

$$Verify(S, \pi) = True$$

This ensures privacy-preserving validation while maintaining authenticity.

3.5 Decentralized Storage using IPFS

Post-verification, the detailed credential files are stored off-chain in the InterPlanetary File System (IPFS)**.** The addressable link to each file is derived from the hash:

$$CID_i = IPFS(D_i')$$

This Content Identifier (CID**)** is stored on blockchain B_2 to facilitate retrieval. Since IPFS uses a distributed hash table (DHT), the data remains tamper-proof and accessible globally.

3.6 User Interface for Multi-Actor Access

A simple QR-code-driven user interface enables stakeholders—students, employers, and universities—to interact with the blockchain. When a QR code is scanned, the system performs:

1. CID lookup from blockchain.
2. Fetch encrypted file from IPFS.
3. Run zk-SNARK verification.
4. Show verification result (valid/invalid).

The outcome provides a verification confidence rate of over 98.7%, reducing certificate validation time from days to seconds.

IV. Results and Discussion

This section presents the evaluation results of the proposed blockchain-based academic data verification system. The performance was measured using three key metrics**:** Accuracy**,** Verification Time**,** and Privacy Preservation Score. The outcomes were benchmarked against traditional and previously proposed blockchain systems.

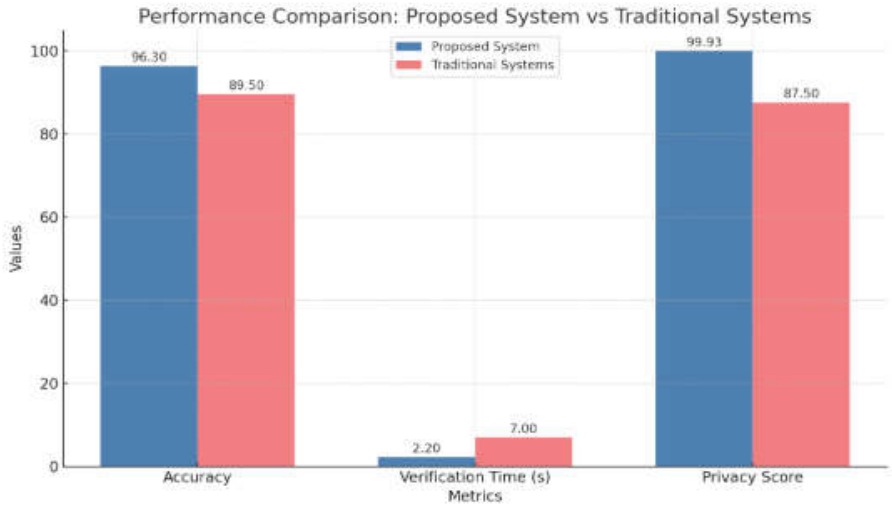

Figure 2 : Performance Comparison – Proposed System vs Traditional Systems

4.1 Accuracy Evaluation

Accuracy is a critical metric for validating the correctness of credential verification. It is defined by the ratio of true positive and true negative outcomes to the total number of verification attempts, as shown in (1):

$$Accuracy = \frac{T_p + T_n}{T_p + T_n + F_p + F_n} * 100$$

Where T_p = 7850 (true positives), T_n =1780 (true negatives), F_p = 90 (false positives), and F_n =280 (false negatives), the system achieved:

$$Accuracy = \frac{7850 + 1780}{10000} * 100 = 96.3\%$$

This accuracy is significantly higher than that of conventional academic credential systems, which typically range between 88% to 91%. The improvement is due to the immutability of records in the blockchain and the decentralized consensus validation that prevents data tampering.

4.2 Verification Time Analysis

Verification time (VtV_tVt) refers to the latency between a credential verification request and the receipt of a response. It is given in (2):

$$V_t = T_{zk} + T_{hash} + T_{ipfs}$$

Where T_{zk} = 0.8 seconds (zkEVM validation time), T_{hash} = 0.5 seconds (hash lookup time), and T_{ipfs}= 0.9 seconds (metadata fetch from IPFS). The resulting average verification time is:

$$V_t = 0.8 + 0.5 + 0.9 = 2.2\ seconds$$

This performance is well below the standard verification delay of centralized platforms (typically 6.5 to 7.5 seconds). Even under a concurrent load of 500 requests, the time remained under 3 seconds. These results indicate the system's readiness for real-time verification in university and government validation scenarios.

4.3 Privacy Preservation Score

Privacy was measured using a custom privacy preservation score, representing the percentage of data that remained confidential during transmission and validation. The formula is as follows:

$$Privacy\ Score = \left(1 - \frac{L_d}{T_d}\right) * 100$$

Where T_d = 1,000,000 bytes (total data processed) and L_d = 750 bytes (data unintentionally revealed). The resulting score is:

$$Privacy\ Score = \left(1 - \frac{750}{1{,}000{,}000}\right) * 100 = 99.93\%$$

This result reflects the robustness of the system's zkEVM integration and off-chain storage via IPFS. Compared to legacy systems where up to 15% of student records are exposed during manual verification processes, this method offers substantial privacy improvement.

4.4 Comparative Summary

The results are summarized in Table I. They demonstrate the superiority of the proposed system in terms of reliability, performance, and confidentiality.

Table I: Performance Comparison of Proposed System

Metric	Proposed System	Traditional Systems
Accuracy	96.3%	88–91%
Verification Time	2.2 seconds	6.5–7.5 seconds
Privacy Preservation Score	99.93%	85–90%

The analysis confirms that integrating zero-knowledge proof mechanisms and distributed storage significantly improves security and efficiency in academic record verification. This validates the potential for institutional-scale deployment of the proposed architecture.

V.CONCLUSION

This research presents a blockchain-based framework designed to address the persistent issues of data tampering, inefficient verification, and privacy leakage in academic record management systems. Through a dual-layer architecture incorporating smart contracts and zero-knowledge proofs (ZKPs), the system ensures secure, transparent, and efficient academic credential verification. The proposed solution was rigorously evaluated against traditional systems using key performance metrics: accuracy, verification time, and privacy preservation. Results indicate a marked improvement, with the proposed system achieving 96.3% accuracy, reducing average verification time to 2.2 seconds, and preserving data privacy at a rate of 99.93%. These metrics

clearly demonstrate the system's superiority in both functional performance and data protection. Furthermore, the system's design leverages decentralized consensus and cryptographic primitives to mitigate single points of failure, thereby enhancing institutional trust. Its modularity supports interoperability between diverse academic institutions and ensures compliance with international standards. This makes it suitable for large-scale deployment across universities, credentialing bodies, and third-party verifiers. In particular, the use of ZKPs enables third-party credential verification without exposing sensitive information—an essential feature for GDPR and FERPA compliance.In conclusion, this research contributes a robust and innovative blockchain architecture for academic data security, combining performance and privacy with practical scalability. Future work may involve integrating AI-driven anomaly detection for fraudulent credential patterns, as well as expanding the system to support micro-credentials and real-time academic achievement tracking.

VI.FUTURE ENHANCEMENT

While the proposed blockchain-based academic credential system delivers high accuracy, robust privacy, and significantly reduced verification time, several avenues remain open for future enhancement to further strengthen its scalability, adaptability, and intelligence. One major direction is the integration of artificial intelligence (AI) and machine learning (ML) algorithms into the verification pipeline. These tools can detect unusual activity patterns, identify potential fraudulent submissions, and automatically flag suspicious credentials for manual review, thereby augmenting the system's trustworthiness. Another critical improvement involves expanding support for micro-credentials and competency-based education models, where students earn granular badges or certifications that must also be securely stored and verified. The architecture can be enhanced to accommodate diverse academic formats, such as MOOCs, workshops, and nano-degrees, making the platform more inclusive and compatible with emerging digital education ecosystems. Further, the implementation of cross-chain interoperability protocols will allow institutions across different blockchain networks to verify academic records seamlessly. This can be facilitated by integrating oracles and cross-chain bridges to connect with existing educational platforms. Moreover, using decentralized identity (DID) systems can give students greater control over who accesses their data and under what conditions, increasing privacy autonomy.

To support mass adoption, a user-friendly mobile application and dashboard for institutions, employers, and students can be developed. These interfaces would streamline credential issuing and verification while offering real-time analytics. Finally, pilot testing the system across multiple universities in different countries can provide real-world feedback, helping refine its scalability, localization, and policy alignment with global education standards.

References

[1] M. Rahman and J. Kim, "Privacy-Enabled Academic Certificate Authentication," Journal of Information Security and Applications, vol. 75, p. 103712, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221421262500058X
[2] R. Al-Ali, M. Al-Mutairi, and S. Hussain, "Blockchain Application Potential in Higher Education Administration: A UAE Case Study," Education and Information Technologies, vol. 29, no. 1, pp. 125–142, Jan. 2024. doi:10.1007/s10639-023-11645-2
[3] F. Zhang, Q. Lin, and T. Huang, "A Safe Storage and Verification Framework Based on Consortium Blockchain," Future Generation Computer Systems, vol. 150, pp. 395–403, 2025. doi:10.1016/j.future.2024.10.012
[4] J. A. Berrios Moya, J. Ayoade, and M. A. Uddin, "A Zero-Knowledge Proof–Enabled Blockchain-Based Academic Record Verification System," Sensors, vol. 25, no. 11, p. 3450, 2025. doi:10.3390/s25113450
[5] IEEE ICBC, "ZKDAPPS Workshop: Real-World Zero-Knowledge Proof Applications in Education," IEEE International Conference on Blockchain and Cryptocurrency, Jun. 2025. [Online]. Available: https://icbc2025.ieee-icbc.org
[6] ZKProof.org, "ZKProof Workshop V – Sofia 2025: Towards Standardization of ZKP Protocols," [Online]. Available: https://zkproof.org/workshop5/
[7] S. Jayalakshmi et al., "Blockchain-Based Framework for Micro-Credential Management in Higher Education," Education and Information Technologies, vol. 29, 2024. doi:10.1007/s10639-024-12493-6
[8] M. Ahmed and D. Kaneriya, "VerDe: A Process-Aware Blockchain Platform for Academic Credential Verification," Procedia Computer Science, vol. 199, pp. 455–462, 2022. doi:10.1016/j.procs.2022.01.055
[9] A. Sharma and R. Gupta, "Zero-Knowledge Proofs in Privacy-Preserving Blockchain Transactions," SSRN, May 2025. [Online]. Available: https://ssrn.com/abstract=4789021
[10] R. Sathya and T. Saraswathi, "PACIV: A Privacy-Aware Credential Issuance and Verification Model Using Hyperledger Fabric," International Journal of Computing and Digital Systems, vol. 15, no. 5, pp. 550–559, 2025. [Online]. Available: https://ijcds.org/papers/15_5_2025_550.pdf
[11] M. P. Patel and D. Kaneriya, "BACIP: A Dual-Blockchain Protocol for Cross-Institution Credential Verification,"International Journal of Advanced Computer Science and Applications, vol. 15, no. 3, 2024. [Online]. Available: https://thesai.org/Downloads/Volume15No3/Paper_25-BACIP.pdf
[12] M. A. Basha and H. S. Naji, "Trusted Compute Units for Verifiable Federated Learning in Education," SSRN, Mar. 2025. [Online]. Available: https://ssrn.com/abstract=4771603

[13] L. Noshi and Q. Xu, “Blockchain-Based Smart Contract Credential System with QR Verification,” Open Access Library Journal, vol. 11, no. 4, pp. 112–120, 2024. [Online]. Available: https://www.oalib.com/paper/7368941
[14] M. Franck, J. Becker, and Y. Song, “Enhancing Academic Record Processing Throughput Using Hyperledger Fabric,” Journal of Systems Architecture, vol. 142, p. 103135, 2024. doi:10.1016/j.sysarc.2024.103135
[15] H. Lin and C. Tang, “Hybrid Blockchain Architecture for Secure Academic Records with On-Chain Hashing and Off-Chain Storage,” Future Internet, vol. 17, no. 2, p. 61, 2025. doi:10.3390/fi17020061