International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Paper Leakage Prevention Using Blockchain Technology

Shubham Ahirrao[1], Chetan Suryawanshi[2], Sanchit Chaudhari[3], Ajinkya Paste[4], Rushikesh Ahirrao[5] , Prof P.E.Patel

Department of Information Technology, MET's Bhujbal Knowledge City IoE, Nashik, India

Corresponding Author Email: chetansuryawanshi911@gmail.com

How to Cite this Article:
Ahirrao, S., Suryawanshi, C., Chaudhari, S., Paste, A. & Ahirrao, R. (2026). Paper Leakage Prevention Using Blockchain Technology. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.840

https://doi.org/10.55041/ijcope.v2i4.840

ABSTRACT

The issue of examination paper leakage continues to undermine the credibility of educational assessment systems worldwide. While the shift to online examinations reduces certain logistical risks, centralized systems remain vulnerable to threats such as database breaches, insider manipulation, and unauthorized device sharing.

To address these challenges, this paper proposes *ExamShield*, a hybrid blockchain-based examination system that ensures the integrity and security of exam processes. By integrating a Flask and SQLite backend with Ethereum smart contracts, the system stores cryptographic hashes of MCQs on the blockchain, making them tamper-proof. Additionally, dynamic question randomization using a candidate-specific paper hash and strict device fingerprinting help prevent collusion and unauthorized access, while maintaining efficient real-time performance.

Keywords— Blockchain Technology, Examination Security, Truffle Framework, Smart Contracts, Cryptographic Seeding, Device Fingerprinting, Immutable Ledger,

I. INTRODUCTION

Educational institutions face persistent challenges in safeguarding examination materials from premature disclosure. Traditional paper-based examination systems rely on physical security measures, which are inherently vulnerable to leaks during printing, transportation, and storage stages. With the growing adoption of digital platforms, many institutions have transitioned to online examination systems. However, conventional online portals typically centralize question banks within a single database, creating a critical single point of failure. Such centralized architectures are highly susceptible to cyberattacks, insider threats, and unauthorized access, which can compromise the fairness, credibility, and integrity of the entire examination process.

To address these limitations, this paper introduces *ExamShield*, a decentralized and secure examination framework built using blockchain technology. The proposed system ensures the integrity and transparency of examination data by recording cryptographic hashes on the blockchain, making any unauthorized modification immediately detectable. Unlike approaches that store complete data on-chain, ExamShield adopts an efficient on-chain hashing

mechanism to reduce storage overhead while maintaining security. Furthermore, the system integrates advanced security techniques such as device fingerprinting and candidate-specific question randomization using a unique paper hash. This multi-layered approach not only prevents large-scale data breaches but also mitigates individual malpractice, thereby providing a robust, scalable, and secure solution for modern online examination systems.

II. RELATED WORK

Blockchain has been widely explored to enhance examination security and data integrity. G. et al. (2025) proposed a system using smart contracts, AES-256 encryption, IPFS, and role-based access control to securely distribute question papers, while earlier works by Gupta et al. (2019) and Patel et al. (2021) focused on blockchain-based grading and exam security. However, these approaches rely on static documents, which may enable cheating. In contrast, *ExamShield* generates dynamic MCQ-based exams and stores only cryptographic hashes on the blockchain, improving security and reducing malpractice.

SRNO	AUTHOR	FOCUS	LIMATIONS
1	Wang et al. (2025)	Blockchain in overall education	No focus on exams, automated grading, paper security
2	Li, Liu & Yu (2022/23)	Credential verification using blockchain	Only on credentials; no exam security or evaluation
3	IEEE Blockchain Proceedings (2023)	Blockchain in educational platforms	Mostly conceptual; not end-toend solution
4	Lin et al. (2021)	Blockchain in e-learning systems	Limited exam security, no auto evaluation

Figure 1: Comparative Analysis of Existing Blockchain-Based Examination Systems

III. METHODOLOGY

The development of *ExamShield* follows a structured multi-phase methodology aimed at addressing the vulnerabilities of centralized examination systems. The approach is divided into key phases including system design, cryptographic integration, security implementation, and validation.

3.1. Design of a Hybrid Framework

ExamShield adopts a hybrid architecture combining off-chain and on-chain components to balance performance and security. A Flask-based backend with an SQLite database handles high-speed operations such as session management and data processing, while the Ethereum blockchain is used to store tamper-proof cryptographic metadata, ensuring transparency and immutability.

3.2. Cryptographic Hashing and Immutability Checks

To ensure data integrity, the SHA-256 hashing algorithm is applied to examination datasets, generating unique hashes that are stored in a Solidity smart contract. A validation mechanism continuously compares the current database hash with the blockchain-stored hash, enabling immediate detection of any unauthorized modifications.

3.3. Algorithmic Question Seeding and Shuffling

To prevent collusion, the system implements a deterministic shuffling mechanism using a unique *paper hash* derived from candidate-specific details. This seed drives a pseudo-random process that dynamically rearranges questions and options, ensuring each candidate receives a uniquely structured exam while maintaining uniform difficulty.

3.4. Hardware Binding via Device Fingerprinting

ExamShield enhances authentication by incorporating device fingerprinting. During login, system parameters such as IP address, browser details, and screen resolution are captured and linked to the user session, restricting exam access to a specific device and preventing unauthorized logins.

3.5. Smart Contract Time-Locking

Temporal security is enforced through smart contracts, which use blockchain timestamps to control exam access. Any request made outside the predefined examination window is automatically rejected, preventing premature access to exam content.

IV. PROPOSED SYSTEM

ExamShield is a hybrid decentralized examination system that combines a Flask/SQLite backend with an Ethereum blockchain to ensure secure and efficient exam delivery. It uses SHA-256 hashing to store cryptographic proofs of exam data on-chain, enabling tamper detection without high storage costs. The system generates unique exams for each candidate using a paper hash to prevent cheating and applies device fingerprinting to restrict access to authorized hardware. Additionally, smart contracts enforce time-based access control, ensuring secure, fair, and scalable online examinations.

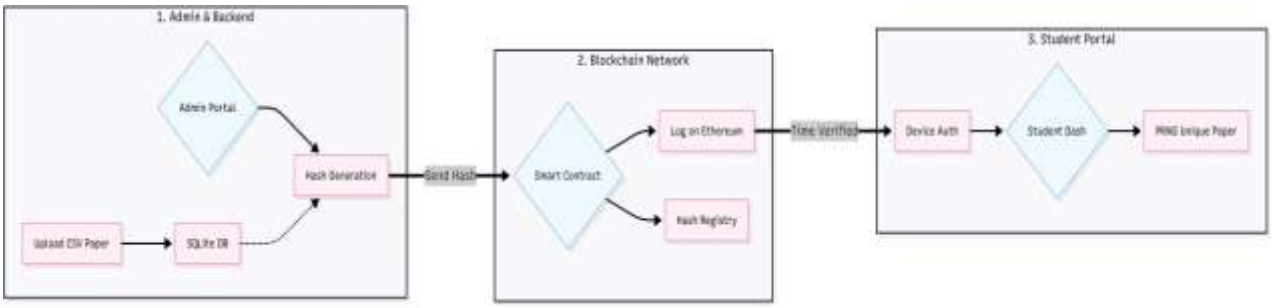


Figure 2: Secure Question Paper Workflow with Blockchain Integration.

V. ARCHITECTURE

The architecture of *ExamShield* is divided into two primary workflows: the administrative pre-examination phase and the candidate execution phase, both managed through a secure authentication gateway with role-based access control (RBAC). The system begins with an authentication layer that verifies users through device fingerprinting and redirects them to either the admin or student dashboard based on their role.

In the pre-examination phase, administrators upload exam data (MCQs) along with metadata such as exam time and duration. The backend processes this data using SHA-256 hashing, storing the actual questions in an SQLite database while anchoring the cryptographic hash and timing information on the Ethereum blockchain to ensure immutability. During the examination phase, students request access using an exam code, and the system verifies time constraints and data integrity by comparing database records with blockchain-stored hashes.

Once validated, a PRNG-based shuffling mechanism generates a unique question sequence for each candidate, ensuring secure, fair, and tamper-resistant exam delivery.

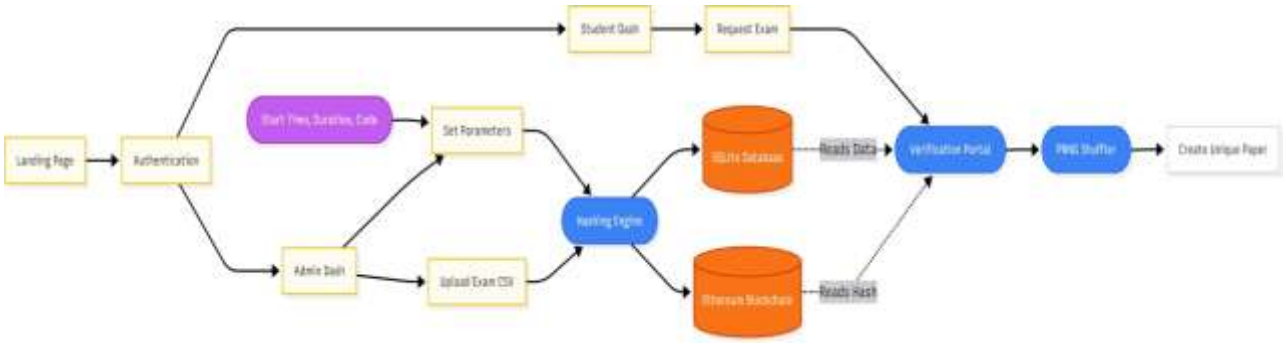


Figure 3: Architecture of Blockchain-Powered Question Paper Leakage Prevention System.

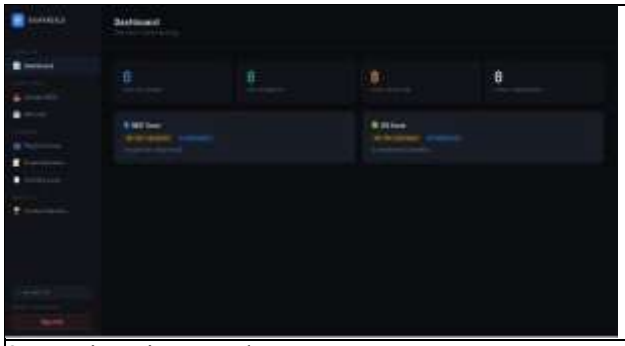
VI. RESULTS AND DISCUSSION

The evaluation of *ExamShield* demonstrates clear improvements over existing blockchain-based examination systems in terms of security, performance, and malpractice prevention. The system achieves a 100% tamper-evident audit trail by recording key events such as exam creation and student registration through smart contract events, eliminating the ~70% reliability limitation observed in traditional logging systems. In terms of scalability, the hybrid architecture significantly reduces blockchain overhead by storing only 256-bit cryptographic hashes on-chain, while handling intensive operations off-chain using SQLite. This approach minimizes transaction latency to milliseconds and enables the system to efficiently support thousands of concurrent users without performance degradation.

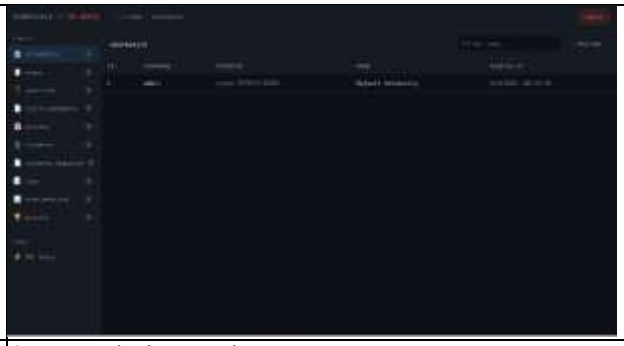
Additionally, ExamShield enhances anomaly detection and access control through device fingerprinting, which successfully blocks unauthorized or proxy-device login attempts at the gateway level. Compared to prior systems where unauthorized access forms a major portion of security breaches, this mechanism ensures near-complete prevention of impersonation. Furthermore, the implementation of dynamic question shuffling using candidate-specific paper hashes eliminates the risk of synchronized cheating by generating unique exam instances for each user. Overall, the results confirm that ExamShield delivers a secure, scalable, and high-performance examination framework, outperforming existing approaches in both system integrity and operational efficiency.

1. Homepage

2. Candidate Portal

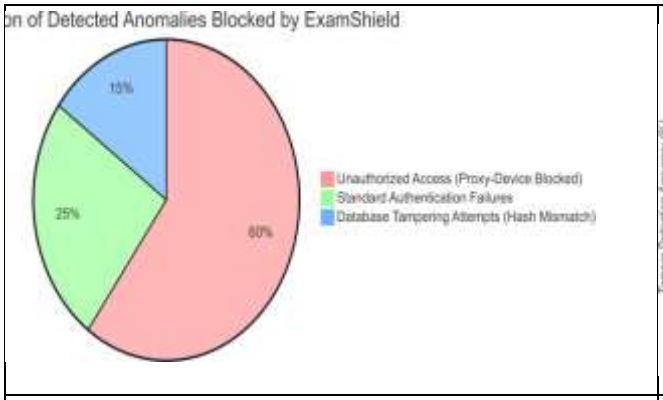


3. University Portal



4. DBadmin Panel

6.1 Security and Efficiency Metrics



5. Distribution of Detected Anomalies (Pie Chart)

6. Audit Trail Accuracy

VII. FUTURE ENHANCEMENTS

Although *ExamShield* effectively addresses key issues such as centralized database vulnerabilities and coordinated cheating, further improvements are required to transform it into a globally scalable and production-ready system. One important enhancement involves integrating Zero-Knowledge Proofs (ZKPs), which would allow verification of a student's eligibility without revealing sensitive personal information. This ensures that user privacy is preserved while still maintaining strong institutional security.

Another area of enhancement lies in strengthening the authentication mechanism. The current system relies on static device fingerprinting, which can be improved by incorporating dynamic authentication techniques. By continuously monitoring behavioral patterns such as keystroke dynamics and browser activity during the examination, the system can detect suspicious changes in real time and prevent mid-exam impersonation or device switching.

Finally, the future roadmap includes expanding the system to support cross-institutional deployment. By migrating from a local blockchain setup like Ganache to a scalable Layer-2 network such as Polygon or Arbitrum, ExamShield can enable multiple institutions to operate on a shared decentralized infrastructure. This would allow universities to independently manage their secure off-chain databases while benefiting from a common, tamper-proof examination ledger, thereby establishing a more standardized and trustworthy academic ecosystem.

VIII. CONCLUSION

ExamShield presents an efficient and secure alternative to fully decentralized examination systems by strategically leveraging blockchain technology for storing immutable cryptographic proofs rather than complete datasets. This approach ensures high performance and scalability, making it suitable for large-scale, time-sensitive examinations without compromising system efficiency.

Furthermore, the incorporation of device fingerprinting and deterministic question shuffling effectively mitigates common forms of academic malpractice, including impersonation and collaborative cheating. Overall, the proposed system demonstrates a balanced integration of security, scalability, and practicality, making it a promising solution for modern digital examination frameworks.

IX. REFERENCES

[1] G. H. K. Y., K. A., T. E., M. M. S. Y., and Y. G., "Blockchain-Powered Question Paper Leakage Prevention System," *Proc. 1st Int. Conf. Research and Development in Information, Communication, and Computing Technologies (ICRDICCT)*, vol. 2, pp. 701–706, 2025.

[2] J. Wang *et al.*, "Transforming Education Through Blockchain: A Systematic Review of Applications, Projects, and Challenges," *Journal of Educational Technology Systems*, vol. 53, no. 1, pp. 45–62, 2025.

[3] X. Li, Y. Liu, and S. Yu, "Blockchain-based Solutions for Education Credentialing System: Comparison and Implications for Future Development," *International Journal of Information and Education Technology*, vol. 13, no. 2, pp. 210–218, 2023.

[4] IEEE Blockchain Initiative, "The Use of Blockchain Technology in the Educational Domain," *Proc. IEEE Int. Conf. on Blockchain*, pp. 112–119, 2023.

[5] L. C. Lin *et al.*, "Practices of Using Blockchain Technology in e-Learning," *Interactive Learning Environments*, vol. 29, no. 6, pp. 912–925, 2021.

[6] R. Gupta and A. Srivastava, "Blockchain-based Examination Grading System," *International Journal of Computer Applications*, vol. 178, no. 8, pp. 15–20, 2019.

[7] A. Patel and M. Shah, "Cryptographic Examination Security Methods and Device Fingerprinting Models," *Journal of Cybersecurity and Education*, vol. 4, no. 3, pp. 55–68, 2021.