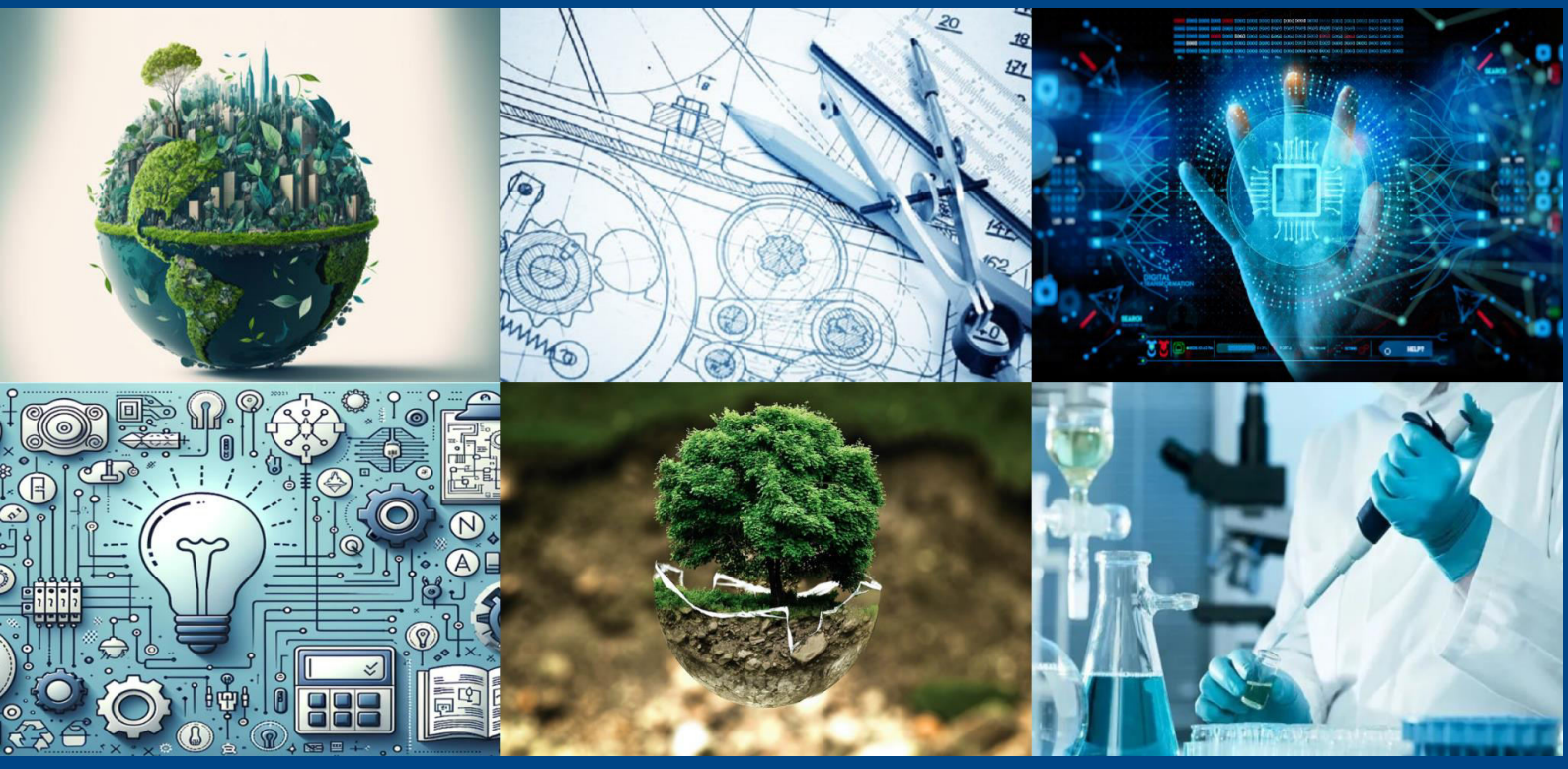
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 5, May 2025**

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805101

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Question Paper Leakage Prevention using Blockchain

Pranathi P

Assistant professor, Dept. of CSE, Shridevi Institute of Engineering and Technology, Tumakur, Karnataka, India

Yojith Siddeshwar G, Laxmi S, Roja G

Dept. of CSE , Shridevi Institute of Engineering and Technology, Tumakur, Karnataka, India

ABSTRACT: The increasing shift toward digital educational systems has magnified concerns surrounding question paper leaks, which compromise academic integrity and undermine institutional credibility. This research proposes a blockchain-based framework specifically designed to prevent question paper leakage by ensuring secure generation, storage, and distribution of exam content. The proposed architecture comprises three core layers: the application layer, the blockchain layer, and the user interaction layer. Leveraging smart contracts, the system automates access control and paper distribution processes, ensuring tamper-proof execution based on predefined conditions. Encryption techniques, time-locked smart contracts, and decentralized file storage through IPFS further fortify security. The performance of the system is evaluated for latency, scalability, and fault tolerance under simulated academic environments. By leveraging the immutable and decentralized nature of blockchain, the framework mitigates risks associated with unauthorized access and manipulation of examination materials. This study highlights blockchain's transformative potential in securing exam logistics, aiming to restore trust and credibility in modern assessment systems. Future research will explore the integration of AI-based intrusion detection and advanced identity verification mechanisms.

KEYWORDS: Blockchain, IPFS, Smart Contracts, Ethereum, Question Paper Security, Immutability, Access Control.

I. INTRODUCTION

The leakage of question papers is a critical issue that continues to plague educational systems globally, often leading to the cancellation of exams, loss of academic integrity, and erosion of public trust in examination bodies [1]. Traditional systems of question paper management are typically centralized, making them vulnerable to internal breaches, unauthorized access, and data tampering during transmission or storage [2,3]. As the education sector increasingly adopts digital platforms, there is an urgent need for a more secure and transparent method to manage sensitive examination content.

Blockchain technology offers a novel and robust solution by introducing decentralization, immutability, and cryptographic security into the examination process [4]. Through a distributed ledger system, blockchain ensures that all interactions and data exchanges are permanently recorded and resistant to unauthorized changes [5]. In the proposed model, question papers are stored off-chain using the InterPlanetary File System (IPFS) to handle large data efficiently, while cryptographic hashes of these files are maintained on-chain to verify data integrity and authenticity [6].

The system employs time-locked smart contracts to control the release of question papers, ensuring they can only be accessed during predefined time windows by authorized personnel or examination centers [7]. This eliminates the risks associated with early or unauthorized exposure. Furthermore, multi-factor authentication (MFA) and role-based access control mechanisms are integrated at the user layer to reinforce access security [8].

By combining on-chain verification with off-chain storage, the framework addresses both scalability and security concerns, enabling institutions to deploy the system across varied exam formats and geographies without compromising performance [9]. Smart contracts also automate key processes like paper generation, encryption, access granting, and distribution logging, thus minimizing human involvement and reducing the risk of insider threats [10,11].

This paper presents a blockchain-enabled system that redefines the approach to securing examination content, providing a transparent and tamper-proof infrastructure to eliminate question paper leaks. The framework promises to enhance trust, accountability, and operational efficiency in examination logistics.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE REVIEW

The issue of question paper leakage has long posed a threat to the integrity of academic examinations, prompting researchers to explore secure technological solutions. In recent years, blockchain has emerged as a promising approach to fortify examination systems against such threats due to its decentralized, tamper-proof, and transparent architecture. Several studies have explored the application of blockchain in online exam environments, focusing on privacy, scalability, and security. For instance, [13] proposed the integration of zero-knowledge proofs with blockchain to protect sensitive data such as question papers and student identities, without compromising the transparency of result verification. Their findings showed that privacy-preserving technologies can coexist with immutable public ledgers, enabling secure data handling.

In a broader educational context, [14] highlighted the utility of blockchain for secure storage and academic credential verification, setting the foundation for its use in examination systems. This was further expanded by [15], who demonstrated the use of smart contracts to automate various academic workflows, including test generation and result publishing. These smart contracts enable deterministic, rule-based automation that enhances both reliability and efficiency.

Building on these initial insights, [16] explored how blockchain could enhance transparency and fairness in examinations. Their study emphasized that once questions are uploaded to the blockchain, they become immutable, preventing any post-creation alterations. Moreover, access controls embedded in smart contracts prohibit unauthorized viewing or editing, thereby securing exam content.

Empirical evidence from blockchain-enabled pilot projects led by [17] indicated a notable reduction in fraud and increased trust in exam administration. These trials illustrated how blockchain's immutability discourages unauthorized changes and fosters confidence among stakeholders.

However, scalability and cost remain major hurdles for mainstream implementation. [18] analyzed Ethereum's performance under high transaction loads typical of mass online examinations. While Ethereum ensured security, high gas fees and transaction latency posed challenges. To mitigate this, the study recommended adopting Layer 2 solutions like zk-Rollups and off-chain storage using IPFS to optimize both cost and performance.

In alignment with these findings, [19] and [20] expanded the scope by integrating privacy-enhancing features within blockchain frameworks. These enhancements were particularly crucial in jurisdictions with strict data protection regulations. Their research proposed a balance between transparency and confidentiality, critical for wide adoption of blockchain-based examination systems.

The potential of AI integration with blockchain was explored by [21], who proposed a hybrid model wherein AI monitors exam sessions for suspicious behavior while blockchain preserves data integrity. Their model allowed AI-triggered smart contracts to flag and respond to anomalies like irregular answer patterns or long inactivity periods, showcasing the synergy between immutability and intelligence.

Further scalability improvements were proposed by [22], who examined consortium blockchain networks. By limiting participation to trusted entities such as universities and exam boards, consortium blockchains reduce gas costs and improve transaction speeds. The study also introduced multi-signature smart contracts, which require multiple verified authorities to authorize actions like question paper distribution, thus reinforcing security and control.

Authentication and identity verification represent another crucial dimension. [23] introduced decentralized identity (DID) systems to ensure secure and self-sovereign verification of student identities. Their model gave users control over personal data, removing the need for third-party verifiers. The use of blockchain to store hashed credentials enabled tamper-proof identity management.

Finally, [24] illustrated how the combination of DID and smart contracts can automate identity verification during exams without compromising privacy. This model enables

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

seamless and secure access to question papers only after confirming the legitimacy of the user, adding another layer of protection against leakage.

A. Scalability

The literature emphasizes the need for scalable blockchain architectures to accommodate high transaction volumes typical of online exams. Ethereum's Layer 2 solutions, such as Optimism and zk-Rollups, have been identified as practical options for maintaining performance during peak loads [18], [26].

B. Public vs. Private Blockchains

While public blockchains like Ethereum provide maximum decentralization and security, they often incur high costs and slower speeds. In contrast, private blockchains (e.g., Hyperledger Fabric) offer better control and efficiency, though with reduced decentralization. The literature underscores the importance of choosing the appropriate blockchain type based on application requirements [25].

C. Performance

To enhance system responsiveness, researchers have advocated for smart contract optimization, off-chain computation, and high-throughput consensus algorithms. Such strategies help in reducing latency and improving user experience [27].

D. Security

Security enhancement techniques identified in the literature include multi-signature wallets, zero-knowledge proofs, and regular audits of smart contracts. These measures prevent tampering, unauthorized access, and data leakage during question paper generation and distribution [28].

E. Reliability

Consensus mechanisms like Proof of Stake (PoS) and redundant storage architectures help maintain system availability and consistency. Distributed networks of nodes reduce single points of failure and ensure continued operation [29].

F. Efficiency

Efficiency improvements are achieved through transaction batching, parallel processing, and gas optimization in smart contracts.

III. MATERIALS AND METHODOLOGY

To implement the proposed model, the following tools and technologies are used:

- **Smart Contract Development:** Solidity
- **Blockchain Platform:** Ethereum (Truffle & Hardhat)
- **Storage Mechanism:** IPFS for storing encrypted question papers
- **Front-End Integration:** Web3.js and MetaMask for secure user interaction

The system implementation follows a multi-stage workflow designed to ensure secure, tamper-proof management of question papers from creation to access:

1. **Encryption and Storage**: The question paper is first encrypted using standard symmetric cryptography to maintain confidentiality. It is then uploaded to the InterPlanetary File System (IPFS), which returns a unique content identifier (CID).
2. **Blockchain Hash Storage**: This CID is stored on the Ethereum blockchain via a smart contract. This ensures that any alteration to the file will change the hash, making tampering evident.
3. **Access Control via Smart Contracts**: Smart contracts are programmed with predefined access conditions, such as time-locks and authorized addresses. These contracts govern when and by whom the question papers can be accessed.
4. **Authentication and Retrieval**: Authorized users (e.g., examination centers) authenticate via MetaMask, which verifies their identity and permissions before granting access to the file's CID from IPFS.
5. **Performance Evaluation**: To assess the system's robustness and efficiency, performance is evaluated on both

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805101

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Truffle and Hardhat frameworks using the following metrics:

- **Gas Consumption**: Measuring the computational cost for executing smart contract functions.
- **Transaction Latency**: Time delay between transaction initiation and confirmation.
- **Success Rate**: Percentage of successful transactions under varying network loads.

This methodology ensures a comprehensive understanding of the system's operational integrity, resource efficiency, and scalability across different Ethereum development environments.

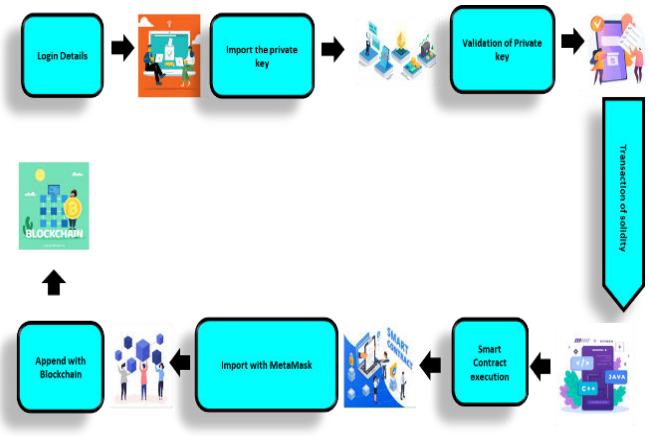


Fig. 1. Architecture Of Ethereum Blockchain for Online Exam

Algorithm

1. Initialize Ethereum environments using Hardhat and Truffle.
2. Deploy smart contracts.
3. Execute operations (Upload QP, Grant Access, Retrieve QP).
4. Measure gas for each action.
5. Compute average gas usage and total framework cost.
6. Calculate percentage gas efficiency.

IV. RESULT ANALYSIS

Sample operations showed that Hardhat outperformed Truffle in gas optimization:

- **TotalGasHardhat** = 327,500
- **TotalGasTruffle** = 350,500

Efficiency (Sample Values):

- Upload QP: 7.92% better with Hardhat
- Access QP: 6.86% better with Hardhat

Transaction visibility and success rates were consistently higher with Hardhat under simulated high-load conditions.

Certainly! Here's an expanded version of the conclusion for “Question Paper Leakage Prevention Using Blockchain”:

V. CONCLUSION

The integration of blockchain technology in the question paper distribution system represents a revolutionary step toward ensuring examination security. Blockchain's decentralized architecture eliminates single points of failure, making it extremely difficult for malicious actors to alter or access sensitive exam data. Its immutability ensures that once a question paper is uploaded to the blockchain, it cannot be modified without detection, thereby preserving its authenticity.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Furthermore, smart contracts can automate access permissions, ensuring that question papers are only released at predefined times to authorized users. This minimizes human intervention and reduces the chances of leaks due to internal collusion or negligence. Blockchain also enables end-to-end traceability, providing an auditable trail of all actions taken on the document — from creation to access and distribution.

Adopting blockchain not only strengthens the technical security of examination systems but also fosters greater trust among students, educators, and administrators. In the long run, this innovation could pave the way for a more secure, transparent, and fair examination ecosystem. Therefore, blockchain holds significant potential to become a cornerstone in combating academic malpractice and ensuring the integrity of educational assessments.

VI. FUTURE WORK

While blockchain offers a strong foundation for securing examination processes, several avenues remain open for future development and enhancement. One important area is the integration of Zero-Knowledge Proofs (ZKPs) and confidential smart contracts to ensure privacy without compromising transparency, allowing secure validation of question papers without exposing their content.

Another direction is the development of a dedicated blockchain platform tailored for educational institutions, which could include modular tools for exam scheduling, question generation, access control, and real-time monitoring. Future systems may also incorporate AI-based anomaly detection to flag suspicious behavior or access patterns across the network.

Furthermore, incorporating interoperability standards could allow different educational boards or universities to collaborate on a unified blockchain infrastructure, promoting a standardized approach to exam security. The use of decentralized identity (DID) systems can further enhance security by ensuring verified access for educators and administrators.

REFERENCES

[1] Canessane, R. A., Srinivasan, N., Beuria, A., Singh, A., & Kumar, B. M. (2019, March). Decentralised applications using ethereum blockchain. In 2019 fifth international conference on science technology engineering and mathematics (ICONSTEM) (Vol. 1, pp. 75-79). IEEE.
[2] Wen, H., Sun, S., Huang, T., & Xiao, D. (2024). An intrinsic integrity- driven rating model for a sustainable reputation system. Expert Systems with Applications, 249, 123804.
[3] Tasic, I., & Cano, M. D. (2024). An orchestrated IoT-based blockchain system to foster innovation in agritech. IET Collaborative Intelligent Manufacturing, 6(2), e12109.
[4] Alagheband, M. R., & Mashatan, A. (2022). Advanced encryption schemes in multi-tier heterogeneous internet of things: taxonomy, capabilities, and objectives. The Journal of Supercomputing, 78(17), 18777-18824.
[5] Choudhury, S., Lenka, R. K., Barik, R. K., & Panda, N. C. (2019, July). Security Protocols in Internet of Things (IoT)-A Review. In 2019 International Conference on Intelligent Computing and Remote Sensing (ICICRS) (pp. 1-6). IEEE.
[6] Darabi, M., & Fathi, A. (2024). Identity Chain. arXiv preprint arXiv:2407.10187.
[7] Zhao, L. (2018). Authentication and Data Protection under Strong Adversarial Model (Doctoral dissertation, Concordia University).
[8] Sorensen, T. (2018). Inter-workgroup barrier synchronisation on graphics processing units (Doctoral dissertation, Imperial College London).
[9] Kumar, S. M., & Manhar, A. (2020). IOT–Overview, Implementation and Upcoming Challenges.
[10] Sorensen, T. (2018). Inter-workgroup barrier synchronisation on graphics processing units (Doctoral dissertation, Imperial College London).
[11] Jain, A., Tripathi, A. K., Chandra, N., & Chinnasamy, P. (2021, January). Smart contract enabled online examination system based in blockchain network. In 2021 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-7). IEEE.
[12] Abdelsalam, M., Shokry, M., & Idrees, A. M. (2023). A proposed model for improving the reliability of online exam results using blockchain. IEEE Access, 12, 7719-7733.
[13] Sattar, M. R. I., Efty, M. T. B. H., Rafa, T. S., Das, T., Samad, M. S.,

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Pathak, A., ... & Ullah, M. H. (2023). An advanced and secure framework for conducting online examination using blockchain method. Cyber Security and Applications, 1, 100005.

[14] Karataş, E. (2018). Developing ethereum blockchain-based document verification smart contract for moodle learning management syst Tsai,

C. T., Wu, J. L., Lin, Y. T., & Yeh, M. K. C. (2022). Design and

development of a Blockchain-based secure scoring mechanism for online learning. Educational Technology & Society, 25(3), 105- 121.em. Bilişim Teknolojileri Dergisi, 11(4), 399-406.

[15] Sun, X., Zou, J., Li, L., & Luo, M. (2021). A blockchain-based online language learning system. Telecommunication Systems, 76(2), 155- 166.

[16] Farooq, M. S., Tehseen, R., & Omer, U. (2021). Blockchain based online examination assessment models for educational institutes: a systematic literature review. VFAST Transactions on Software Engineering, 9(3), 57-67.

[17] Deenmahomed, H. A., Didier, M. M., & Sungkur, R. K. (2021). The future of university education: Examination, transcript, and certificate system using blockchain. Computer Applications in Engineering Education, 29(5), 1234-1256.

[18] Sholeh, M., Talahaturuson, E. Y., Rizqi, M., & Gumelar, A. B. (2022). Designing an Ethereum-based blockchain for tuition payment system using smart contract service. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 6(2), 275-280.

[19] Kulkarni, M. D., & Alfatmi, K. (2021, June). New approach for online examination conduction system using smart contract. In 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT) (pp. 848-852). IEEE.

[20] Shukla, A., Patel, N., Tanwar, S., Sadoun, B., & Obaidat, M. S. (2020, October). BDoTs: Blockchain-based evaluation scheme for online teaching under COVID-19 environment. In 2020 International Conference on Computer, Information and Telecommunication Systems (CITS) (pp. 1-5). IEEE.

[21] BouSaba, C., & Anderson, E. (2019, April). Degree validation application using solidity and Ethereum blockchain. In 2019 SoutheastCon (pp. 1-5). IEEE.

[22] BouSaba, C., & Anderson, E. (2019, April). Degree validation application using solidity and Ethereum blockchain. In 2019 SoutheastCon (pp. 1-5). IEEE.

[23] Xue, L., Fu, R., Lin, D., Kuok, K., Huang, C., Su, J., **&** Hong, W. (2021). Exploring the innovative blockchain-based application of online learning system in university.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com