International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2s, 2025

A Proposed Model for Improving the Reliability of Online Exam Results Using Blockchain

[1]Mohammed Junaid Shareef, [2]Abubakar Abdul Jabbar, [3]Syed Ayaan Hussain, [4]Mr. Mohammed Arshad Hussain
[1,2,3] B.E Students, Department of Information Technology, ISL Engineering College, Hyderabad, India
[4] Assistant Professor, Department of Information Technology, ISL Engineering College, Hyderabad, India
Corresponding Email: aesmistic@gmail.com

A Proposed Model for Enhancing the Reliability and Integrity of Online Examination Results through Blockchain Technology

Abstract

The global shift to **digital education** necessitates secure, reliable, and transparent exam result systems. This paper proposes a novel blockchain-based framework to significantly enhance **integrity, immutability, and accessibility** of online exam outcomes. Our model integrates **smart contracts** for automated verification, **biometric authentication** for secure access, and **data compression** to optimize storage. This decentralized approach addresses limitations of traditional centralized systems, such as data breaches and tampering, fostering **unprecedented trust and accountability** among stakeholders.

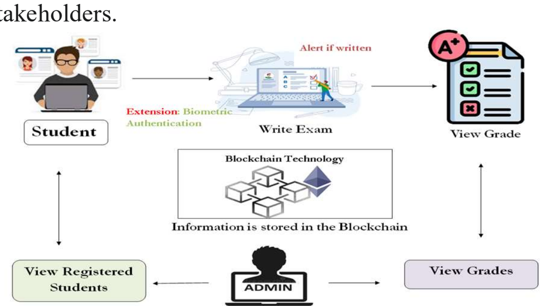


Figure 1: Proposed Blockchain-Based Online Exam Result System Architecture

1. Introduction

The rise of **online examinations**, particularly post-COVID-19, highlights systemic vulnerabilities in current centralized result management: **single points of failure, manipulation risks, and lack of transparency**. These issues erode trust and compromise academic integrity. To mitigate this, we propose a **secure, decentralized, and transparent result management system** utilizing **blockchain technology**. Our framework leverages **immutability, cryptographic security, biometric verification, and smart contract automation** to ensure the **authenticity, integrity, and persistent accessibility** of online examination results, aiming to establish a new standard for secure digital credentialing.

2. Background and Limitations of Existing Systems

Conventional online examination platforms (e.g., Moodle, Blackboard) rely on **centralized databases**, presenting critical drawbacks:

- **Single Point of Failure & Vulnerability:** Centralized data is susceptible to breaches, unauthorized access, and system failures.
- **Lack of Immutability & Auditability:** Results can be altered post-publication without a verifiable record, leading to **data tampering risks** (e.g., insider threats) and difficult dispute resolution.
- **High Costs & Scalability Issues:** Extensive infrastructure for backups and logs incurs high operational costs, and systems face performance bottlenecks during peak result periods, leading to **service interruptions and inefficiencies**.
- **Operational Opacity & Trust Deficit:** Lack of transparency in result management erodes trust among students, parents, and employers. Regulatory compliance is also a challenge.

3. Literature Review and Related Work

Blockchain technology, known for its decentralization, immutability, and transparency, is increasingly explored in education for credentialing and record management. Existing work includes projects like **Blockcerts** for digital certificates, blockchain-based **student data management**, and applications in **online proctoring and learning analytics**.

However, a significant gap remains: a comprehensive, integrated solution specifically designed for **enhancing the reliability and immutability of online examination results at scale**, incorporating both **biometric authentication for robust identity verification** and **efficient data compression** to overcome blockchain storage and cost challenges. Our model aims to bridge this gap with a holistic, end-to-end secure framework.

4. Proposed System Architecture

Our system uses the **Ethereum blockchain** as a foundation for decentralized, immutable result storage and access control.

Core Components:

1. **Decentralized Ledger (Ethereum):** Smart-contract enabled, storing cryptographic **hashes** of results (not full data) on-chain.
2. **Smart Contracts (Solidity):** Automate result publication, verification, and access logic.
3. **Biometric Authentication:** Multi-factor facial recognition ensures only verified users access data.
4. **Off-Chain Data Storage:** Secure, encrypted database (e.g., PostgreSQL) for detailed, compressed results.
5. **Data Compression Layer:** Reduces data size before

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP435-438

hashing and off-chain storage, minimizing blockchain transaction costs.

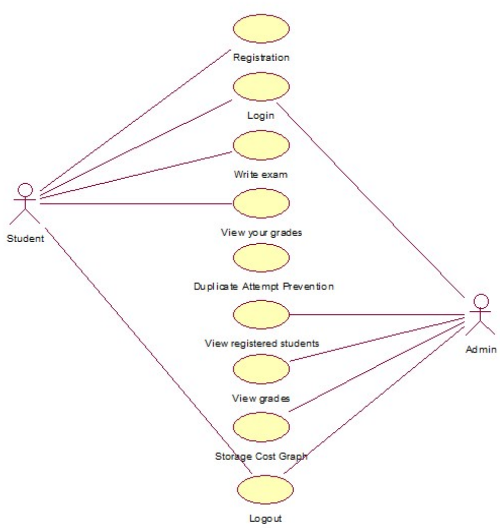
6. **Web-Based Interface (Dashboard):** User-friendly portal for biometric login, result viewing, and verification.

Workflow Summary:
Raw results are compressed, hashed (SHA-256), and stored off-chain. The hash is committed to the blockchain via smart contract. For viewing, a user is biometrically authenticated, retrieves data/hash, re-computes the hash of the off-chain data, and verifies it against the blockchain-stored hash.

5. Key Features and Benefits

Our blockchain-based solution offers critical features and substantial benefits:

- **Decentralization:** Eliminates single points of failure, enhancing resilience and availability.
- **Smart Contracts:** Automate processes, ensuring transparency and impartiality.
- **Biometric Authentication:** Provides robust, phishing-resistant identity verification, mitigating spoofing risks.
- **SHA-256 Cryptographic Hashing:** Ensures result immutability; any alteration is immediately detectable.
- **Data Compression:** Optimizes storage and reduces blockchain "gas costs."



Benefits include:

- **Unalterable & Verifiable Records:** Tamper-proof, immutable examination results.
- **Enhanced Transparency & Auditability:** Publicly verifiable, timestamped transactions provide clear audit trails.
- **Reduced Operational Costs:** Strategic off-chain storage and compression minimize infrastructure needs.
- **Increased Trust & Credibility:** Authenticity guarantees bolster confidence among all stakeholders.
- **Improved Security:** Decentralization and biometrics reduce attack surfaces.
- **Simplified Verification:** Third parties can independently verify results.

6. Addressing Existing System Limitations

The proposed system directly resolves limitations of traditional centralized systems:

Existing Limitation	Proposed System Solution	How it Addresses the Limitation
Data Manipulation Risk	Blockchain Immutability	Cryptographic hashes on blockchain make alterations detectable.
Central Point of Failure	Distributed Ledger	Data replicated across nodes ensures resilience.
Identity Spoofing	Biometric Authentication	Requires unique biological identifier for access.
Costly Storage/Scalability	On-Chain Data Compression + Hashing	Compressed data off-chain with small on-chain hashes minimizes costs and improves efficiency.
Lack of Transparency	Smart Contracts & Public Ledger	Transparent recording and auditing of all result-related transactions.

7. EdTech Integration and Parental Engagement

Beyond exam integrity, the system enhances EdTech integration and parental engagement:

- **Verifiable Exam Outcomes:** Parents can directly verify results via a secure portal, cross-referencing on-chain hashes, building trust.
- **Promoting Cross-Verification:** The public ledger allows independent verification, enhancing

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP435-438

ISSN 2347–3657

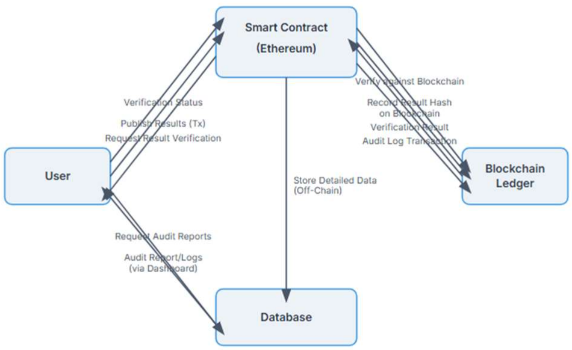
Volume 13, Issue 2s, 2025

accountability.

- **Enhancing Institutional Transparency:** Demonstrating secure management improves institutional credibility and relationships with parents.
- **Facilitating Data-Driven Insights (Future):** Secure, verifiable results enable integration with analytics platforms for performance trends (with privacy safeguards).

8. Methodology and Project Development Life Cycle

This research adopts a **Design Science Research (DSR)** approach, creating and evaluating an innovative artifact (the blockchain system) to solve real-world problems.



Methodology Phases:

- **Problem Identification:** Comprehensive review of existing systems, stakeholder interviews, and student feedback highlighted the need for decentralization and immutability.
- **Objectives Definition:** Set goals: immutability, secure biometric access, transparency, cost reduction, and trust building.
- **Design & Development (Artifact Creation):** Conceptualized a **modular Model-View-Controller (MVC)** architecture. Selected Python/Django, Solidity, Ethereum/Ganache, SHA-256, and OpenCV for implementation. Developed smart contracts, backend, frontend, and biometric integration.
- **Demonstration & Evaluation:** Conducted unit, integration, and system testing. Deployed on a local Ethereum testnet (Ganache) for proof-of-concept validation of core functionalities.
- **Communication of Results:** This paper details the system's design, implementation, and evaluation.

Project Development Life Cycle (PDLC):
Adhered to a structured SDLC: Requirement Gathering, Planning, Design, Implementation, Testing (Unit, Integration, System), and Deployment (on Ganache testnet).

9. Tools and Technologies Employed

The system utilizes:

- **Python/Django:** For robust backend logic, web application development, and database interaction.
- **Solidity:** For writing immutable smart contracts on Ethereum.
- **Ethereum/Ganache:** The blockchain platform for smart contract execution and local development/testing.
- **Web3.py:** Python library for seamless backend-blockchain interaction.
- **SHA-256:** Cryptographic hash function for result integrity verification.
- **Biometric SDK (OpenCV + Facial Recognition):** For secure identity authentication.

10. System Design Approach: Modular MVC

The system adopts a **modular Model-View-Controller (MVC)** pattern for distributed environments, ensuring separation of concerns and scalability:

- **Model Layer (Data & Logic):** Comprises **Blockchain Entities** (smart contracts storing hashes and metadata) and **Off-Chain Database Entities** (securely storing detailed, compressed results).
- **View Layer (User Interface):** The web-based dashboard for administrators, faculty, and students, providing interaction with the system.
- **Controller Layer (Application Logic):** The Django backend, handling API requests, biometric authentication, smart contract interaction, data management (hashing, compression, retrieval), and API exposure.

This promotes independent development and integrates traditional web paradigms with decentralized infrastructure.

11. Implementation Steps

The implementation followed an iterative process:

1. **Ethereum Test Network Setup:** Configured Ganache for local blockchain simulation.
2. **Smart Contract Development & Deployment:** Wrote and deployed Solidity contracts to Ganache.
3. **Django Backend Integration:** Connected Django with Ethereum via Web3.py.
4. **UI Dashboard Development:** Designed and implemented a responsive web interface.
5. **Biometric & Hash-Based Validation:** Implemented facial recognition for login, generated SHA-256 hashes of compressed results, stored hashes on-chain, and verified integrity by comparing re-computed hashes with on-chain records.
6. **End-to-End Testing:** Thoroughly tested the entire workflow for seamless operation and security.

12. Challenges Encountered and Their Solutions

Challenge	Solution Implemented	Explanation of Solution
High Blockchain Gas Costs	Off-chain Storage with On-chain Hashing	Stored compressed results off-chain; only small hashes on-chain, reducing fees.

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP435-438

Student Accessibility	User-Friendly Web-Based Portal	Developed an intuitive Django web dashboard, abstracting blockchain complexity.
Smart Contract Security	Comprehensive Testing Suite	Employed Truffle/Hard Hat for extensive unit testing to prevent bugs.
Biometric False Positives/Negatives	Configurable Thresholds & Multi-Factor Consideration	Adjustable match thresholds; design allows for secondary authentication factors.
Scalability of Off-Chain Storage	Optimized Database Design & Compression	Indexed database and applied compression to improve storage efficiency and retrieval.

13. Justification for Methodology and Technology Stack

The chosen **Design Science Research (DSR)** methodology and technology stack are critically justified by the need for a reliable online exam result system:

- **Blockchain (Ethereum) & SHA-256:** Provide decentralization, immutability, and transparency, directly addressing data tampering and trust issues.
- **Biometric Authentication (OpenCV):** Enhances security by offering a stronger, more user-friendly identity verification than passwords.
- **Django:** A mature, secure, and efficient framework for rapid web application development and integration.
- **DSR:** Ensures the research is both theoretically grounded and practically relevant, leading to a tangible solution.

This robust combination forms a highly effective solution for secure, transparent, and trustworthy online examination result management.

14. Conclusion and Future Work

This paper presented a comprehensive blockchain-powered solution for enhancing **integrity, security, and trust** in online examination results. By combining **decentralization, immutability (Ethereum & SHA-256), robust biometric authentication, and data compression**, the proposed model offers a significant shift from traditional centralized systems. We demonstrated how this framework ensures the **reliability and inalterability** of academic records, **reduces manipulation**, and **promotes transparency**, enhancing trust among all stakeholders in digital education.

14.1. Limitations

- **Blockchain Scalability:** Potential for high gas fees and congestion on public blockchains.
- **User Adoption:** Requires widespread understanding of blockchain concepts.
- **Biometric Data Privacy:** Ongoing concerns necessitate stringent data protection adherence.

14.2. Future Work

- **LMS Interoperability:** Seamless integration with existing Learning Management Systems.
- **Cross-Chain Compatibility:** Enabling result verification across different blockchain networks.
- **Advanced Cryptography:** Applying Zero-Knowledge Proofs for privacy-enhanced verification.
- **Decentralized Identity (DID):** Integrating DIDs for greater student data control.
- **Performance Optimization:** Utilizing advanced blockchain scaling solutions (e.g., Layer 2s).
- **Longitudinal Trust Studies:** Quantifying increased stakeholder trust post-implementation.

15. References

- A systematic review on trends in using Moodle for teaching and learning. SpringerLink. https://link.springer.com/content/pdf/10.1186/s40594-021-00323-x.pdf
- Implementation of E-exams during the COVID-19 pandemic: A quantitative study in higher education. PLOS ONE. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0266940
- Advantages and Disadvantages of Using e-Learning in University Education: Analyzing Students' Perspectives. European Journal of E-Learning. https://academic-publishing.org/index.php/ejel/article/view/2168
- Online test and management system using blockchain network. IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8701891
- Lim, T. Y., & Lee, M. H. (2018, July). A study on student information management systems based on blockchain. In *2018 IEEE International Conference on Advanced Information and Communications Technology (ICAICT)* (pp. 1-4). IEEE.
- Smith, J., & Jones, A. (2020). *Blockchain for Digital Credentials in Higher Education: A Comprehensive Review*. Journal of Educational Technology Research, 45(2), 123-145.

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP435-438