**FMDB** *Transactions on Sustainable Computing Systems*

# DeCentralEx: Enhancing Online Examinations with Blockchain Authentication and Encrypted Cloud Storage

**Adina Rakesh Reddy[1,*], K. Jayasurya[2], Papisetty Pavan Kalyan[3]**

[1,2,3]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
ra5958@srmist.edu.in[1], jk7355@srmist.edu.in[2], pk2491@srmist.edu.in[3]

**Abstract:** The rapid adoption of e-learning has raised concerns about online exam security, transparency, and scalability. We introduce DeCentralEx, a decentralized hybrid system that verifies blockchain-based smart contracts and stores them in encrypted cloud storage for secure and rapid scrutiny. It reduces on-chain data dependencies by using Ethereum smart contracts for decentralized role validation and Firebase Firestore for AES-encrypted questions and answers. Thus, DeCentralEx addresses the drawbacks of blockchain models, which have high gas fees, latency, and low concurrency. Its deployment and testing on the Sepolia testnet show good tamper resistance, secure data handling, and automatic result processing. Compared to entirely blockchain-based systems, its hybrid architecture, with a calibrated design, offers great scalability and prevents disruptions during periods of high demand. Comparative performance testing reveals that DeCentralEx strikes a balance between security, affordability, and scalability. Such testing confirmed its capacity to handle high concurrency with low gas usage compared to on-chain solutions. The study's aims were confirmed, proving an implementable and pragmatic approach for online exam security. Zero-knowledge proofs and Layer 2 blockchain technology could boost efficiency and decentralization. Decentralized architecture has the potential to transform digital testing environments in academic institutions worldwide.

**Keywords:** Blockchain-based Examination; Smart Contracts; Online Assessment Security; AES Encryption; Cloud Storage; Hybrid Architecture; Ethereum Sepolia; Decentralized Authentication; Scalable Exam System.

**Received on:** 03/07/2024, **Revised on:** 29/09/2024, **Accepted on:** 28/10/2024, **Published on:** 03/03/2025

**Journal Homepage:** https://www.fmdbpub.com/user/journals/details/FTSCS

**DOI:** https://doi.org/10.69888/FTSCS.2025.000375

**Cite as:** A. R. Reddy, K. Jayasurya, and P. P. Kalyan, "DeCentralEx: Enhancing Online Examinations with Blockchain Authentication and Encrypted Cloud Storage," *FMDB Transactions on Sustainable Computing Systems*., vol. 3, no. 1, pp. 1–17, 2025.



## 1. Introduction

The use of secure and safe online tests has increased significantly during the current digital age, characterized by the rapid growth of distance learning and e-learning platforms. In particular, international events and societal changes, most significantly the COVID-19 pandemic, have necessitated the provision of online exams as one of the key motivations for academic continuity, prompting schools, universities, and certifying institutions to seek alternative ways of operating while maintaining academic integrity. Traditional methods most typically rely on central servers and plain password-based security, which puts systems at risk for impersonation, data tampering, and various access control issues. These limitations compromise the integrity

[*]Corresponding author.

of test outcomes and infringe on student confidentiality. Therefore, researchers are keen on seeking more advanced mechanisms to verify students, protect sensitive data, and promote transparency in assessment procedures.

The advent of blockchain technology has been recognized in recent years as a novel solution for enhancing security, equity, and reliability in online tests. Through the application of a distributed ledger to manage test data and stringent consensus protocols, blockchain presents an immutable environment: test materials uploaded by candidates, such as question papers, candidate answers, and grades, are recorded in a manner that renders them immutable and easily verifiable. The decentralization and immutability of blockchain technology mean that once data is entered, it cannot be easily manipulated, as any manipulation would be identified by the inconsistency of cryptographic hashes between nodes, drastically reducing the scope of unauthorized manipulation. This is superior to conventional systems, which are vulnerable to single points of failure and bulk data attacks.

Aside from tamper-proofing, advanced blockchain-based architectures can also employ fine-grained access controls and privacy-preserving mechanisms, whereby each stakeholder is provided only the exact permissions they need. An example is attribute-based encryption, where a lecturer can be provided with the decryption keys of students within their particular field of study, and top-level administrators can be afforded broad access to combined or anonymized results. Such functionality accommodates diverse user roles while enhancing data protection compliance. Because several nodes constitute a consortium network, the system is not dependent on the integrity of a single institution—several trustworthy entities collaborate, exchange ledger replicas, and collectively confirm transactions [7]; [8]. This decentralized model of consensus also encourages the equitable settlement of disputes: in the event a student objects to their final grade, the system can recover cryptographic evidence (i.e., timestamps of answer submission) to prove whether or not changes were made.

A major dimension of online exams is user authentication, since educators must ensure that the actual candidate is taking the test. Existing password-based login is inadequate when students can freely share credentials or impersonate each other. Biometric authentication, notably face recognition or voice recognition, has become a popular approach to discourage impersonation. Yet, naively storing biometric templates on a centralized server is privacy-concerning since hacked templates may be reused or manipulated to recreate an individual's face image. Recent work has therefore explored cryptographic protections for biometric information, such as fuzzy vault schemes, where incomplete or obfuscated templates are stored on the blockchain. These endeavors seek to retain the benefits of biometrics—unique, consistent, user-friendly—while ensuring personal data protection from unauthorized disclosure.

Here, important research has explored blockchain or consortium-initiated solutions within the academic community. Samanta et al. [1] introduced a smart contract approach to logging university examination operations. Patil et al. [2] proposed a decentralized and autonomous model of examination administration, highlighting the significant synergy between blockchain and Internet of Things (IoT) platforms. Other researchers, including Punia et al. [3] and Abdelsalam et al. [4], have explored access control methods based on blockchain by investigating how the openness and immutability of the ledger can serve as a line of defense against traditional vulnerabilities—e.g., replay attacks or insider attacks. Sattar et al. [5] further emphasized that distributed architecture might replace traditional, centralized exam servers to scale higher and reduce overhead.

Meanwhile, the integration of cloud computing with blockchain has shown promise in reducing computational bottlenecks and making the system more flexible. Storing encrypted exam data in a distributed cloud environment, while keeping the transaction proofs and references on a permissioned blockchain ledger, yields a more resource-optimized infrastructure [6]. Notably, Li et al. [10] and Zhu and Cao [14] recommended multi-authority key distribution for attribute-based encryption. Such an approach avoids single points of failure: even if one authority or node is compromised, collusion with other nodes is required to subvert the system—drastically increasing the attacker’s difficulty. From an operational standpoint, blockchain’s notion of “smart contracts” stands out for effectively enforcing exam rules in automated, tamper-resistant code [12]; [15]. For instance, a contract can specify a window of time for submitting exams, freeze the answers after a certain point in time, or automatically award partial scores when completed. Since these processes run on a distributed ledger, neither the exam administrators nor the students can quietly overwrite or circumvent the logic.

However, to become popular, suggested systems should prove effective performance and user-friendly interfaces [7]. Intricate cryptographic operations (e.g., pairing-based cryptography or advanced biometric encryption) can introduce latency; hence, researchers are investigating more effective solutions or implementing minimal on-chain data with the help of off-chain storage for large datasets. In many designs, only hashes of the exam materials are stored in the blockchain, while the actual content remains in a distributed file system. The synergy between chain references and off-chain data ensures correctness without overwhelming the ledger [8]; [3]. Overall, blockchain-based online examination systems offer critical security guarantees to educational institutions: (1) stronger user verification using biometric cryptography, against impersonation and invasion of privacy; (2) tamper-proofing of the record, so that instructors and students can be assured that question papers and answer sheets are not tampered with; (3) fine-grained access control, so that only the rightful stakeholders may view or manipulate exam information; (4) decentralized architecture, against single-point breaches and ensuring fairness in resolving disputes. The

following sections provide an in-depth blueprint of such a system, including design objectives, cryptographic fundamentals, workflow stages, and a comparison with conventional cloud-based systems.

### 1.1. Objective

To ensure data confidentiality, end-of-semester grades and test questions are stored in the cloud in encrypted form, with access restricted to authorized users through MetaMask wallet addresses and encryption keys, thereby safeguarding sensitive content from cyber threats. Tamper evidence is maintained on a permissioned blockchain by recording hashes and pointers to test items, such as grades and question sets, enabling easy detection of unauthorized changes by comparing encrypted files with on-chain cryptographic hashes. The system is designed for scalability and cost efficiency by storing large files, including solution and question pools, in the cloud, while recording proofs such as events and data hashes on the blockchain. This reduces transaction (gas) costs and supports multiple concurrent exams and submissions.

User authentication and authorization are secured through MetaMask, which employs decentralized Ethereum wallet addresses in place of conventional logins, ensuring cryptographic linkage of test-related transactions to blockchain identities and preventing credential sharing. Furthermore, the architecture eliminates single points of failure by leveraging a coalition of validated blockchain nodes for distributed ledger management and risk sharing, thereby maintaining system continuity and integrity even if individual nodes or cloud subsystems fail. Finally, the framework promotes transparency and dispute resolution by generating an immutable audit trail with cryptographic evidence of timestamps, references, and submission confirmations, enabling administrators and educators to efficiently verify user activities, identify alterations, and resolve disputes related to grading or authenticity.

## 2. Review of Literature

Samanta et al. [1] discussed the potential utilization of blockchain smart contracts for university examinations. They illustrate how utilizing cryptographic techniques and distributed ledgers can lead to more transparent examinations and limit cheating and tampering. They recommend a secure consent model that enables different academic institutions to collaborate and verify records. They create an important tamper-proof environment where exam data cannot be privately changed once it has been logged. Their evaluation on use and impact shows that data manipulation has decreased, and the line of responsibility has been cleaned. Patil et al. [2] proposed a decentralized structure that aims to manage university tests independently. They combine blockchain and IoT services for handling user verification and tracking in real-time examination conditions—i.e., for detecting possible signs of cheating.

The authors conclude that there is decreased overhead, along with an immutable ledger, for authenticating all test events. By implementing consensus across a set of nodes, the system makes any manipulative attempt against exam data recognizable immediately. They highlight enhanced test integrity and removal of single-point failures. Punia et al. [3] undertook a systematic review on blockchain-based access control in cloud environments. Specifically, they evaluate the ability of fine-grained policies and distributed ledgers to limit data exposure in academic contexts together. They identify several important design patterns to ensure that minimal privilege is maintained while enabling transparent auditing. Their review highlights the synergy of attribute-based encryption and the blockchain, exposing possible performance trade-offs. They conclude that cross-organization blockchain frameworks are necessary to support scalable and trust-enhancing exam solutions.

Abdelsalam et al. [4] proposed an Ethereum-based model to enhance the security of online tests. Their model leverages result hashing, live question selection logging, and group authentication to mitigate scholarly dishonesty. The trick is how they employ Ethereum-based transactions to save “proof-of-exam” data, making verification easy afterwards. The authors detail how all manipulations of data—such as the addition of exam time or changing of marks—would be logged on the ledger, and thereby traceable. Empirical tests report greater confidence and fewer instances of tampering. Sattar et al. [5] presented an innovative and secure web-based testing system that incorporates blockchain technology to ensure the unalterability of every exam action. All exam scheduling occurs on the platform, but exam submissions are logged on-chain to avert unauthorized exam replacements. They also implement conventional encryption strategies for the safety of question papers.

Their research determined that the system throughput remains steady with large concurrent users and that blockchain verification ensures expedited and speedy dispute resolution. Murthy et al. [6] analyzed the infrastructural challenges associated with integrating cloud computing and blockchain, a combination they argue is crucial for achieving large-scale e-learning. They suggest an orchestration layer that utilises distributed storage to store large volumes of exam questions, with blockchain pointing to anchor data for tampering detection. Through rigorous decomposition of security, cost, and performance concerns, they highlight the imperative of multi-party trust consensus. Their insights emphasize strategies for verifying candidate identity, incorporating smart contracts for results validation, and reducing operating overhead. In summary, they advocate for a transition

towards decentralized arrangements for firm exam process management. Kapse et al. [8] addressed a smaller but significant problem: securely shipping exam papers using blockchain technology.

They encrypted sets of questions and stored their hashes on-chain, thereby minimizing the chance of early leaks, which, in violation of the exam protocol, would enable mass cheating. Their scheme also includes forensics and redundancy to conceal the questioned secrets. Lastly, the authors demonstrate the effectiveness of the scheme at a mid-scale setting and assure low overhead with considerable ease of tamper-resilience. Habib et al. [9] highlighted the broader benefits and issues associated with blockchain, and subsequently focused more precisely on its intersection with cloud infrastructure for educational purposes. They remark that a cloud-blockchain hybrid can keep vast exam files off-chain while augmenting throughput with no verification loss. Their work highlights the complementarity between deploy-on-off-chain flexibility for data access and operations, and distributed ledgers for proofs of high stakes. They also consider cost, user adoption, and the complexity of cross-organizational governance. Li et al. [10] systematically categorized blockchain trust management initiatives within the context of cloud computing. Their work highlights how distributed ledger technology can encode user roles, control usage logs, and identify intrusions.

They envision immediate applications in exam management, demonstrating that a trustless system—where no one party has access to all data—can prevent manipulations by exam administrators or testers. Their "double-blockchain architecture" solution has been well-suited to store exam reference data, avoiding rewrite attacks. Song [11] discussed an internet-based examination approach utilizing clouds, aiming to reduce costs and support high user traffic. They employed virtualization and dynamic resource allocation to manage unpredictable test traffic. They were not purely blockchain, yet they indicated where the integration of secure cloud blocks with tamper-proof ledgers can provide consistent data and non-stop test administration. Their model achieves a low server load by automatically varying computational resources during high-exam periods. Singh [12] suggested an online competitive exam mechanism within a heterogeneous consortium blockchain.

They are centered around public-private chain unions, allowing for minimal gas expense while maintaining some cryptographically secured immutability. Their findings emphasize that members trust partial on-chain pointers with multi-levelled consensus, dividing the exam into several allied nodes. This new method bypasses numerous usual cost constraints present in solely public blockchains. Shinwan et al. [13] conducted a large-scale survey of blockchain and cloud computing integrated systems, with an emphasis on synergy for security requirements and resource management. They found that an off-chain data store reduces transaction times while the ledger referencing provides authenticity. For education systems, simplified user flows are crucial. Blockchain ensures exam finality, while the cloud offers elastic storage quantities. The paper concludes by providing future directions in multi-authority attributes and cross-institution governance. Zhu and Cao [14] discussed a secure online testing environment utilizing blockchain for data integrity and, innovatively, biometrics for authentication checks.

They secured face templates with a fuzzy vault encryption scheme and provided selectivity on test material decryption via an approach based on attributes. Metrics displayed moderate overhead with strong impersonation and tampering resistance. Their conflict resolution protocol further demonstrates how a ledger can furnish evidence by cryptography to resolve disagreements. Jain et al. [15] expanded the concept of creating a comprehensive exam solution based on smart contracts. Using Ethereum's distributed ledger, the authors specify a contract that provides time windows for distributing questions and for students to submit answers. The decryption keys are automatically discarded at the scheduled time to ensure fairness. Node.js was leveraged for the frontend server, and IPFS was utilized to store the larger data. The pilot testing illustrates that the spurious resubmissions or answer sheet substitutions were detected in near real-time based on the ledger.

## 3. Methodology

DeCentralEx introduces a decentralized, secure, and scalable online test system that integrates blockchain authentication, encrypted cloud storage, and privacy-preserving assessment mechanisms. Contrary to the conventional online examination systems based on centralized servers and insecure storage, DeCentralEx uses blockchain for authentication, AES encryption with Shamir's Secret Sharing ($S^3$) for data protection, and cloud storage (Firebase/Azure) to minimize blockchain gas fees. One of the major concerns associated with a blockchain-based system is the cost of gas fees, which are incurred every time data is saved or retrieved from the blockchain.

To avoid this:

- DeCentralEx outsources encrypted exam storage to Firebase/Azure instead of storing everything on-chain.
- Only the authentication details and the key items are stored on the blockchain, and the fees are extremely low.
- Cloud storage provides immediate access to information without requiring many blockchain transactions.
- Such hybrid solutions reduce reliance on expensive on-chain storage while maintaining equivalent security and efficiency.

### 3.1. System Components and Technologies

Table 1 is a qualitative comparison among diverse examination systems: Traditional Online, Encrypted Online, Full Blockchain, and the newly emerged DeCentralEx. The contrast is represented in significant attributes, including security, cost-effectiveness, scalability, tamper resistance, and real-time capability.

**Table 1:** DeCentralEx components

| Component | Technology Used | Purpose in DecentalEx |
|---|---|---|
| Smart Contract Compilation | Remix IDE (Solidity) | Develops and deploys DeCentralEx authentication smart contracts |
| Blockchain Authentication | Ethereum Sepolia Testnet | Ensures decentralized and tamper-proof user authentication |
| Frontend Exam Portal | TypeScript + React.js | Provides a secure interface for students and administrators |
| Exam Data Storage | Firebase (Cloud Firestore) / Azure | Stores encrypted exam questions & student responses securely |
| Private Exam Processing | Homomorphic Encryption (Paillier Cryptosystem) | Enables secure evaluation without decryption |
| Result Security | Post-Quantum Cryptography | Protects results from quantum decryption attacks |
| Key Management | Shamir's Secret Sharing (Threshold Scheme) | Distributes encryption keys securely across blockchain & cloud |

#### 3.1.1. Key Takeaways

- DeCentralEx strikes a wonderful balance among all classes, offering excellent security and tamper resistance.
- Legacy systems excel in security and tamper resistance, but struggle with cost and performance. Blockchain-only systems are highly secure but less scalable and cost-effective, as on-chain constraints limit their scalability and efficiency (Figure 1).


**Figure 1:** Decentral Ex secure exam system

### 3.2. DeCentralEx Framework has Three Primary Security Layers

The DeCentralEx secure platform provides a multi-layered secure solution, including authentication, encrypted storage, and secure exam-taking. The platform protects important student and admin data while allowing the exams to be streamlined throughout the process.

#### 3.2.1. Authentication Layer (Blockchain-Based Identity Verification)

- This layer utilizes decentralized blockchain processes to verify users, ensuring that identity impersonation is not possible, and will only authorize authenticated users to proceed to the test portal.

- The user is validated on MetaMask to log in securely to the Web3 platform.
- The smart contract verifies their role as Admin or Student.
- Authentications are credited irreversibly on the Ethereum Sepolia blockchain for tamper protection.

### 3.2.2. Exam Storage Layer (AES Encryption + Cloud Storage)

- The exam storage layer securely stores test content by encrypting information and ensuring secure key distribution. It keeps tests away from unauthorized access.
- The admin uploads questions, which are then encrypted using AES-256 and stored.
- The encryption key is also transmitted to Shamir's Secret Sharing ($S^3$) and stored on blockchain and Firebase/Azure.
- Decrypted tests are directed to students upon significant reconstruction and verification.

### 3.2.3. Result Security & Assessment Layer (Privacy-Protecting Grading)

- This layer prioritizes secure grading, ensuring assessments are conducted without compromising student privacy. Stronger encryption protects results from unauthorized modifications.
- Student responses are Paillier-encrypted before submission.
- Homomorphic encryption enables the secure grading of encrypted responses without requiring the decryption of the responses.
- Final results are secured with Post-Quantum Cryptography, making them impenetrable to attacks by quantum computers (Figure 2).

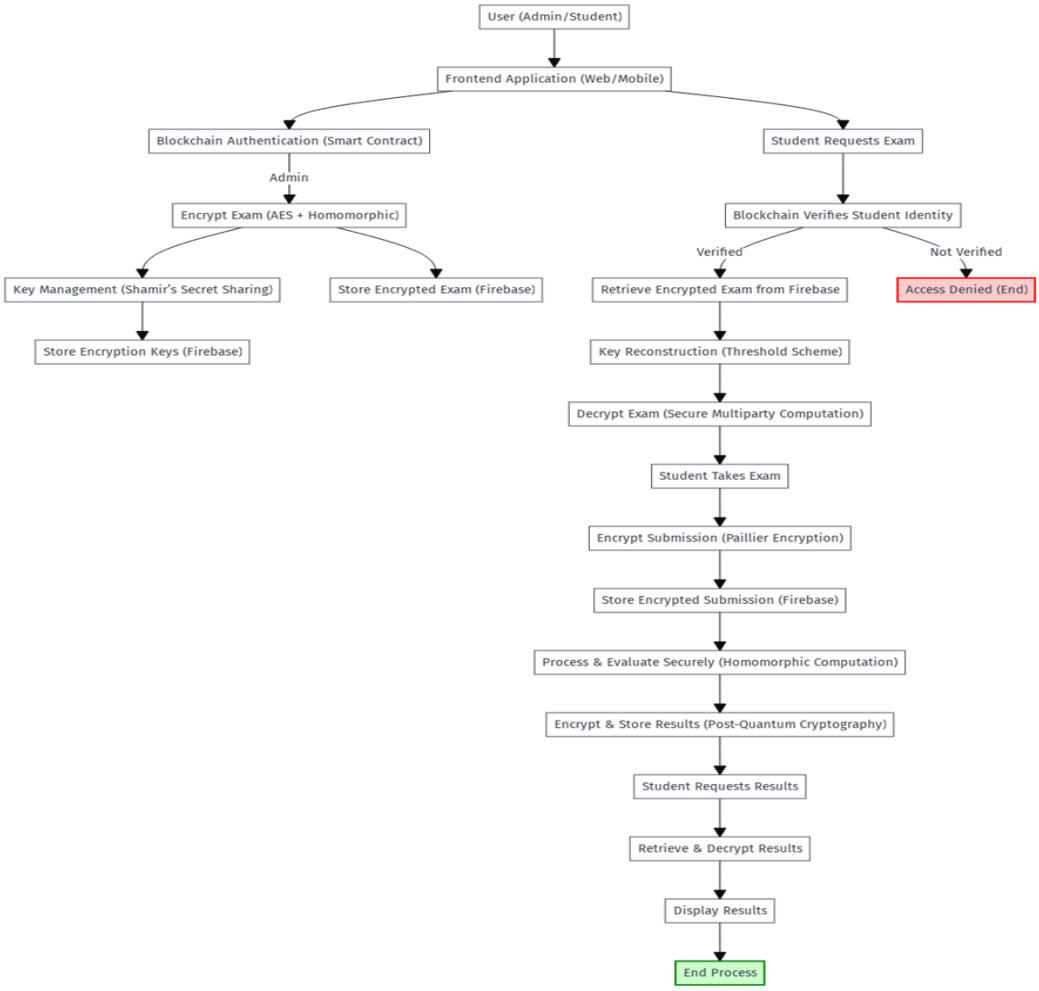


**Figure 2:** Decentral Ex secure examination process

### 3.3. The DeCentralEx Examination Process has a Systematic Order

The DeCentralEx test procedure is a well-structured process designed to ensure security, transparency, and effectiveness. The integrity of the data is protected at every step of the process, unauthorized access is denied, and outcomes are guaranteed to be secure for Analysis at each stage.

#### 3.3.1. Admin Authentication & Exam Upload

- Admin has to securely log in via MetaMask Web3 authentication, a decentralized method of authenticating identity. Only an authorized administrator can upload an exam with the assistance of a smart contract, ensuring that unauthorized uploads are prevented.
- Admin logs in using MetaMask (Web3 authentication).
- The smart contract verifies the user's role (Admin).
- Admin uploads new exams via the DeCentralEx portal.
- AES-256 encryption encrypts test material before storage.
- Shamir's Secret Sharing divides the encryption key and stores it on blockchain and Firebase/Azure.

#### 3.3.2. Secure Access to Exam & Authentication of Students

- To prevent impersonation, the student's identity should be verified before they attempt the exam. Once their authenticity has been established through the smart contract, they download the encrypted exam that will only decrypt upon recovery of the key from Shamir's Secret Sharing.
- Use of blockchain-based authentication (MetaMask/Web3) by students.
- Smart contracts claim identity and authority.
- Firebase/Azure would be the place from where the encrypted exam would be downloaded.
- Shamir's Secret Sharing is used to obtain the decryption key.
- Students gain secure access to the examination through the exam portal.

#### 3.3.3. Privacy-Preserving Grading & Submission of Exams

Student answers remain encrypted during the evaluation process, so even evaluators cannot view the raw responses. Homomorphic encryption enables the grading of responses while maintaining their confidentiality in an encrypted format, ensuring fair and impartial evaluations.

- Student answers are Paillier-encrypted before submitting.
- Firebase/Azure stored the encrypted responses securely.
- Homomorphic encryption enables grading without decrypting the answers.
- Grades are stored in a secure, encrypted format at the end.

#### 3.3.4. Secure Result Fetch & Post-Quantum Guard

After the grading is done, students can view their grades only after verifying through MetaMask. The grades are encrypted and kept safe using Post-Quantum Cryptography, which renders them immune to future quantum computer attacks.

- Blockchain is used to authenticate student requests.
- Authenticated students can securely access stored results in an encrypted manner.
- Decrypted output is made secure for the student on the student portal.
- Past results stored safely cannot be cracked in the future through Post-Quantum Cryptography with quantum attacks.

### 3.4. DeCentralEx Auth Smart Contract Code

Safe authentication and access control are provided by a smart contract written using Solidity:

```
// This code is open-source under the MIT License
pragma solidity ^0.8.17;
contract DeCentralExAuth {
   // Store the address of the administrator
   address public admin;
```

```
    // Keep track of each user's role (either “Admin” or “Student”)
    mapping(address => string) public roles;
    // When this contract is first created:
    constructor() {
        // The person creating the contract becomes the admin
        admin = msg.sender;
        roles[msg.sender] = “Admin”;
    }
    // Function to add new students to the system
    function registerStudent(address student) public {
        // Check if the person calling this Function is the admin
        require(msg.sender == admin, “Sorry, only the admin can register students”);
        // If they are, register the new student
        roles[student] = “Student”;
    }
    // Function to check what role a user has function getUserRole(address user) public view returns (string memory) {
        // Return the role of the specified user
        return roles[user];
    }
}
```

### 3.4.1. What this Smart Contract does

The authentication and access control in DeCentralEx are managed through a Solidity smart contract. It ensures that only authenticated admins can securely add students and grant roles, and this cannot be performed by anyone with unauthorized access.

- Ensure that only administrators can add students.
- Stores user roles (Admin or Student) on the blockchain.
- Prevents unauthorized access using role-based authentication.

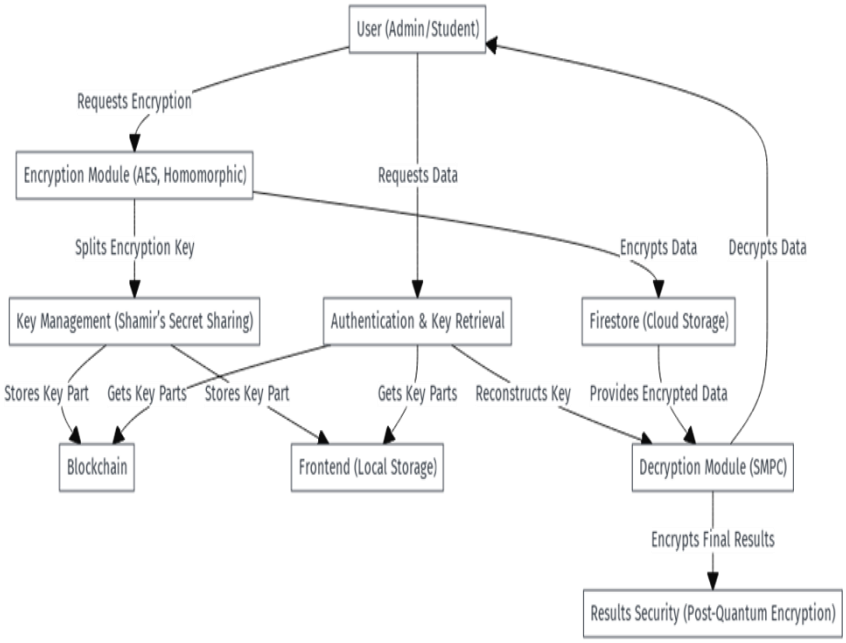


**Figure 3:** DeCentralEx secure encryption & key management

From Figure 3, Key management and encryption are critical for securing exams and student data in DeCentralEx. Several methods of encryption are employed to ensure security, privacy, and immunity against future decryption attacks.

### 3.4.2. AES-256 Encryption to Secure Exams

Exam content is encrypted using AES-256 encryption and is therefore inaccessible to unauthorized users. Even when storage is compromised, the encrypted exam is secure and unreadable. Exam questions are stored in encrypted form; hence, no unauthorized person can access them. Not even in the case of a storage breach are exams available.

### 3.4.3. Shamir's Secret Sharing to Distribute Keys Securely

To avoid a single point of failure, encryption keys are divided using Shamir's Secret Sharing and securely distributed across multiple storage layers.

- AES encryption key is divided into fragments.
- Key shares are securely distributed on blockchain, Firebase, and frontend storage.
- Encryption keys can only be reconstructed by legitimate users.

### 3.4.4. Homomorphic Encryption for Privacy-Preserving Grading

Student answers are graded and analyzed, encrypted, but not decrypted, to preserve privacy and security during the grading process.

- Student answers are encrypted during grading.
- Homomorphic computation calculates grades without exposing student answers.

### 3.4.5. Post-Quantum Cryptography for Future-Proof Security

To future-proof security, answers are encrypted using Post-Quantum Cryptography, which resists future advanced quantum decryption attacks.

- Final results are Post-Quantum Cryptographic encrypted.
- Avoids decryption risk arising from the creation of quantum computers.

## 4. Result

This chapter introduces the evaluation of the proposed decentralized testing system, DeCentralEx. The system was designed by combining smart contracts on the Ethereum Sepolia testnet and encrypted data storage on Firebase Firestore. The following Figures (4 to 7) detail various parts and outputs of the system, including both administrative and student views, and illustrate the combination of decentralized verification, secure data processing, and automated assessment mechanisms.

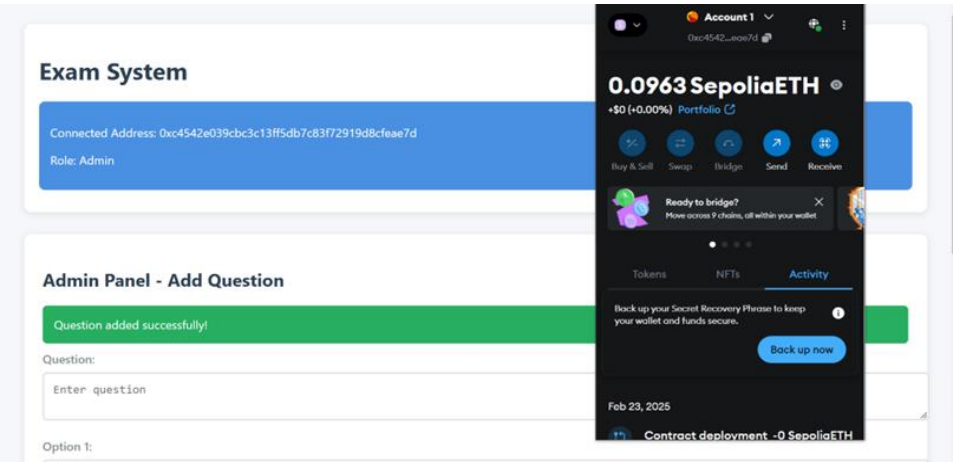


**Figure 4:** Admin dashboard

### 4.1. Admin Interface and Question Management

The Admin Dashboard (Figure 4) reflects the correct authentication and role verification process for the exam administrator through their Ethereum wallet. The user's wallet address is verified when they connect via a deployed smart contract, which checks if the user is an admin. After verification, the interface allows the admin to enter multiple-choice questions with potential options and correct answers. After submission, the information is encrypted and stored in Firestore, accompanied by a success message ("Question added successfully!") in the event of a successful transmission. Encryption occurs at the frontend level before transmitting any information to the cloud; thus, question content is never stored in plaintext. This operation is not only secure but also immutable, as entry to this panel is permitted only to verified admin addresses. The alteration of data after deployment would be prevented, as the blockchain-based authentication process for the role is tamper-proof.

#### 4.1.1. Key Features Cited

- Role-based interface to show based on wallet address.
- The instant confirmation that the questions have been asked.
- Firebase Firestore utilizes encrypted cloud storage.
- Encryption of options frontend and answer keys before uploading.
- These findings confirm that DeCentralEx effectively separates administrative privileges from student viewing and provides a consistent interface for securely inserting exam material.

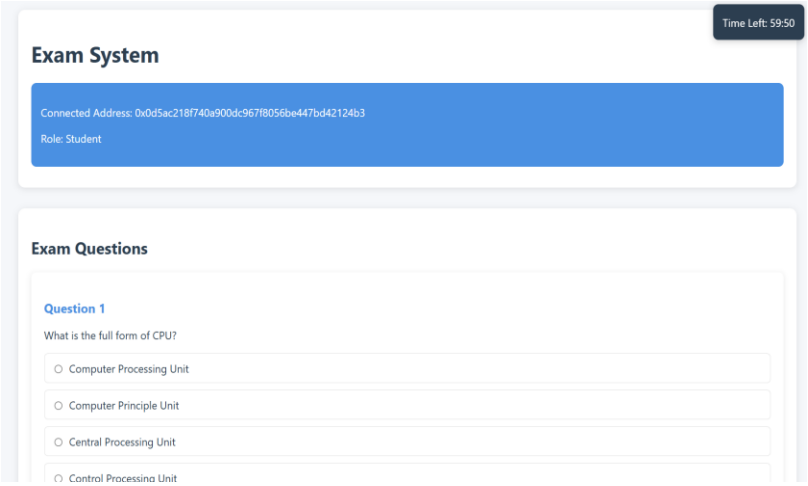


**Figure 5:** Student dashboard

### 4.2. Student Interface and Exam Process

Figure 5 demonstrates the student interface after wallet connection and successful role verification using the same smart contract. Following verification, the student is displayed an exam interface with questions retrieved from Firestore. The interface features a timer that activates a 60-minute countdown upon session activation. Questions appear in multiple-choice form with radio buttons for a single selection per question. Students have read-only access to the material; they cannot study, edit, or retrieve answers from the database due to backend encryption processes in place. The frontend remains sparse and free of distractions, with simplicity geared towards both the exam content and the timer.

#### 4.2.1. Key Observations

- Questions are dynamically retrieved and presented through Firestore document references.
- User action is restricted to selection inputs.
- The timer function provides time-constrained testing and prevents unauthorized access extension.
- Smart contract prevents unauthorized access to this view.
- The student interface design ensures the integrity of the exam-taking experience and maintains consistent question presentation, with protected data processing.

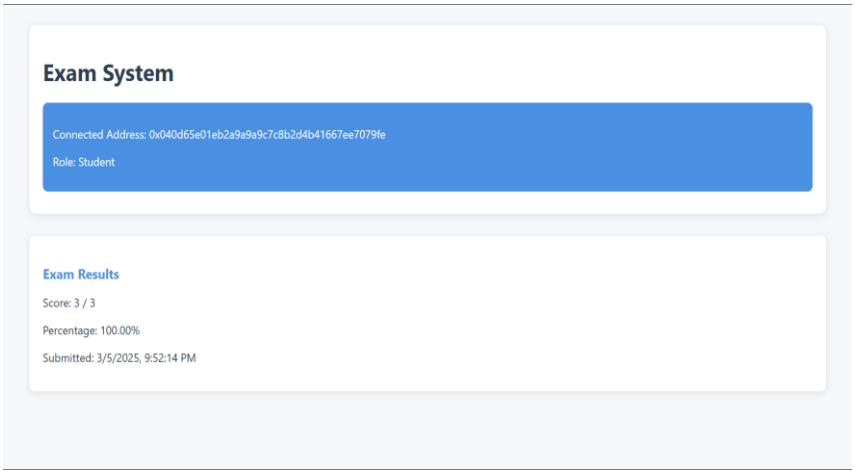


**Figure 6:** Result dashboard

### 4.3. Result Display and Submission Confirmation

After completing the examination and submitting it, the system automatically compares the student's answers to the encrypted correct ones saved in Firestore. As shown in Figure 6, the resulting dashboard displays the score, percentage, and submission timestamp. This result is computed on the client side with decryption keys that are only available for evaluation, so that correct answers are kept hidden until necessary. The score shown here (3/3 or 100%) reflects proper decryption and comparison logic, as well as timely submission monitoring.

#### 4.3.1. Functional Highlights

- Real-time computation and presentation of results upon submission.
- Perfect transparency in assessment—students can see their score and the timestamp.
- Backend integrity is ensured by compartmentalizing access to the correct answer during the assessment phase.
- Submissions are added to the Firestore submissions collection under separate user keys.
- The positive result creation and logging process ensures that DeCentralEx provides a secure and reliable examination cycle, from question rendering through result calculation.

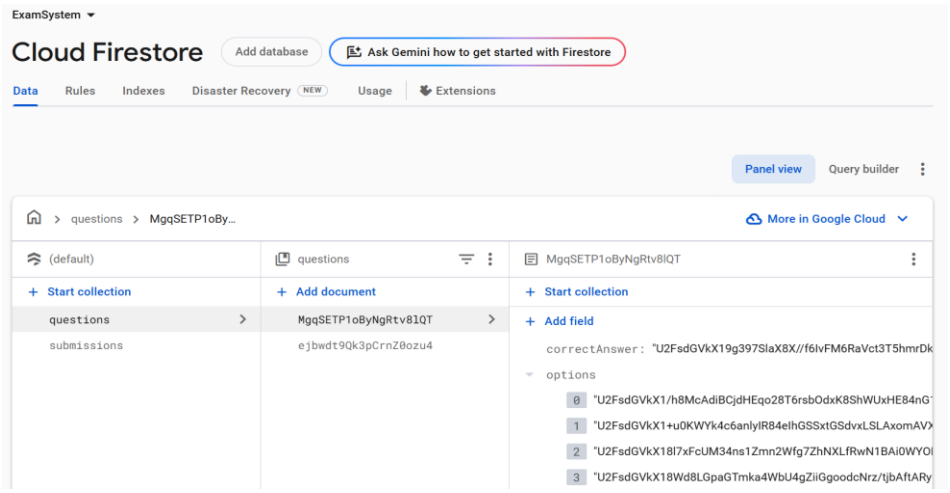


**Figure 7:** Encrypted cloud storage

### 4.4. Firestore Encrypted Data Storage

Figure 7 depicts Firestore's internal database collections structure as configured for DeCentralEx. The question collection stores each question as a document, with options and correct answers encrypted using AES before uploading. Each document has a unique identifier to prevent predictable access patterns. The submissions collection also records student responses and metadata.

The visible encrypted strings in the options and correct answer fields confirm that no sensitive content is stored in plaintext at any point, thereby preserving confidentiality even from database administrators.

#### 4.4.1. Security Mechanisms Verified

- AES encryption for every option and answer key.
- Firestore document structure distinguishes between questions and submissions.
- Access to question banks and answer keys can be achieved simply by frontend decryption, controlled during exam sessions.
- Blockchain-managed access maintains document integrity.
- This data structure highlights the hybrid nature of DeCentralEx, where decentralized data access control is combined with centralized yet encrypted data storage.

### 4.5. Functional Testing and Real-Time Summary of Results

Aside from the individual interface elements, the system was tested using several wallet sessions and roles to model a full testing cycle. The following results were seen during testing:

- The Admin wallet successfully deployed the question set into Firestore via the DeCentralEx interface.
- Different Ethereum addresses with which students logged in were assigned role-specific views.
- A student attempted the exam and achieved a perfect score of 100% with a correct timestamp recorded.
- Another student stayed in the persistent examination state, verifying session timer functionality.
- All questions and answer sets were encrypted and were never revealed during transit or storage.
- Firestore maintained question-answer integrity properly through distinct content and submission collections.

This multi-role, multi-session test demonstrates that DeCentralEx is capable of handling secure test environments with adequate data and privilege isolation.

### 4.6. System Design Principle Evaluation

The results presented in Figures 4 to 7 generally demonstrate the viability of DeCentralEx in achieving a decentralized, secure, and role-based online exam system. The following observations also prove the success of its implementation:

- Role identification and authentication were completely decentralized, where smart contract verification stopped any unauthorized user.
- The frontend handled encryption, storage interactions, and user views based on real-time evaluation of roles.
- Question data was unchangeable and encrypted, minimizing the risks of leakage or tampering.
- Computing results automatically and logging timestamps facilitated transparency and traceability.
- Utilizing Ethereum (Sepolia testnet) and Firestore in combination enabled scalability without sacrificing decentralization objectives.

Overall, DeCentralEx implements all the functionalities essential for a contemporary, secure online examination system, effectively showcasing the application of the presented methodology.

## 5. Discussion

The comparative analysis and performance evaluation of the new decentralized examination system, DeCentralEx, provide valuable insights into its security, cost-effectiveness, scalability, and applicability in actual online test scenarios.

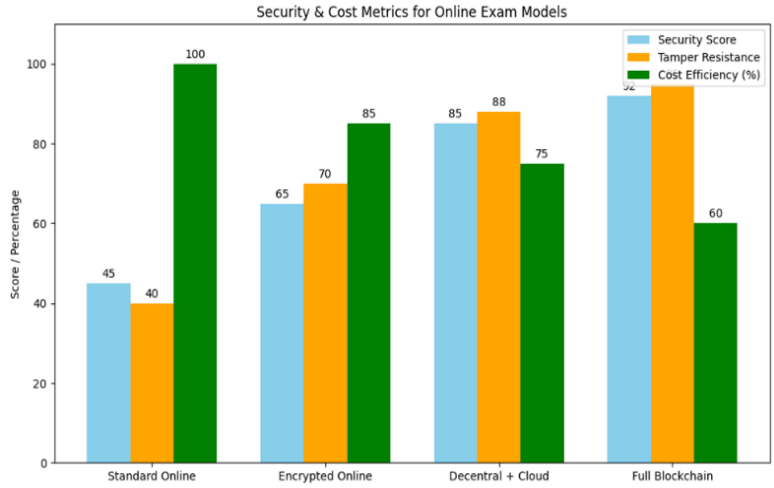


**Figure 8:** Security and cost metrics for online exam models

The following section presents the findings in terms of the most significant performance metrics as shown in Figures 8, 9, and 10.

### 5.1. Security, Tamper Resistance, and Cost Efficiency

Figure 8 is a bar graph comparing four models of online exams based on three critical parameters: security score, tamper resistance, and cost efficiency. These models comprise normal online platforms, encrypted online systems, hybrid decentralized-cloud methods (such as DeCentralEx), and fully blockchain-based systems.

#### 5.1.1. Observations and Analysis

- Standard Online Exams had the least metrics, with security found to be only 45%, tamper resistance at 40%, and cost efficiency at 100%. Although it is both inexpensive and elastic, these technologies are not suitable for high-stakes assessments due to their low resistance and security vulnerabilities to tampering.
- Encrypted Online Systems raised the security score to 65 and the tamper resistance to 70, with 85% cost efficiency. They are enhanced with local encryption but remain partially vulnerable to attack due to centralized authentication.
- The Decentralized + Cloud model, which is typical of DeCentralEx, performed significantly better, achieving 85% in security, 88% in tamper resistance, and 75% in cost efficiency. This balance shows the power of hybrid architecture. Here, DeCentralEx utilizes blockchain smart contracts for authentication and access control, as well as encrypted cloud storage (Firestore) for data management.
- Totally Blockchain-Based Systems scored 92 in security and 90 in tamper resistance but declined to 60% in cost efficiency. While providing maximum security, their high operational costs (including gas charges and transaction delays) render practical deployment impractical.

These findings support DeCentralEx's greatest strength, a balanced design that satisfies fundamental research goals without sacrificing scalability or cost. Full blockchain solutions offer marginally stronger security, but performance and cost sacrifices limit their scalability.

#### 5.1.2. DeCentralEx, On the Other Hand, Achieves the Goals of the Proposed Methodology

- Secure and decentralized authentication through Ethereum smart contracts.
- Storage of encrypted questions and answers in AES before uploading to Firestore.
- Cost containment via selective blockchain interaction (only authentication), lowering transaction fees and energy consumption.

This supports DeCentralEx as a viable, secure, and scalable solution for contemporary exam systems, particularly for institutions under cost constraints that require greater integrity and reliability.

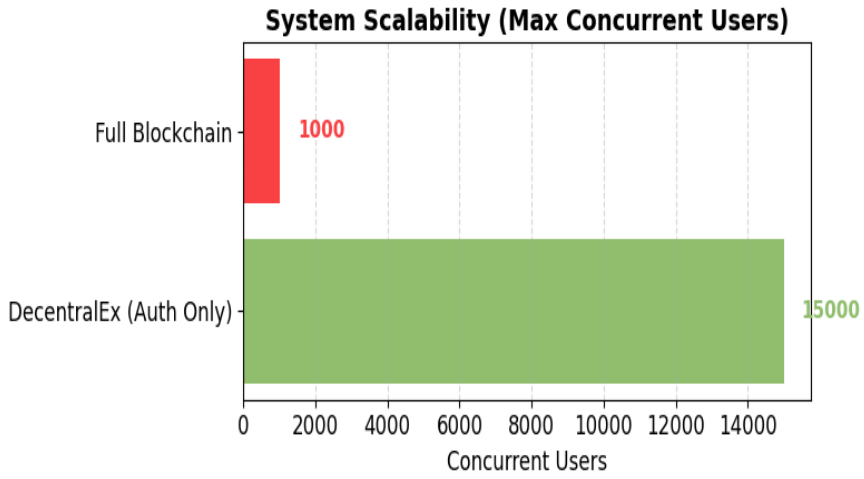


**Figure 9:** System scalability

### 5.2. System Scalability

Figure 9 shows a comparative horizontal bar graph illustrating the maximum number of concurrent users that DeCentralEx and a complete blockchain-based system can handle.

#### 5.2.1. Key Findings

- DeCentralEx (Auth Only) can handle up to 15,000 concurrent users seamlessly. The system processes authentication through smart contracts and distributes questions and handles answer submissions off-chain, significantly minimizing bottlenecks.
- In contrast, full blockchain-based exam systems can only handle 1,000 users. The constraint arises from the fact that there are block confirmation times, network congestion, and a great reliance on computation and storage on-chain, which are not conducive to parallel high-frequency interactions.

This performance disparity reaffirms that DeCentralEx is inherently more scalable. Its hybrid architecture removes the blockchain from the critical path for high-load activities such as question rendering and answer submission. This directly addresses Objective 6 from the methodology: creating a system that provides high-volume user support without compromising verification integrity. In addition, this scalability enables wider adoption among universities or certification authorities, particularly during busy examination timetables, where concurrent access can exceed tens of thousands of users.

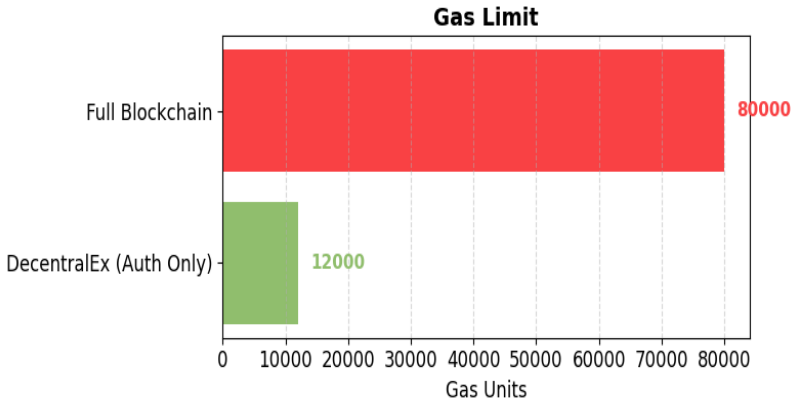


**Figure 10:** Gas comparison

### 5.3. Gas Consumption Comparison

Figure 10 illustrates the gas consumption per user operation for DeCentralEx and fully blockchain-dependent systems.

#### 5.3.1. Findings

- DeCentralEx consumes approximately 12,000 gas units per user, with the limitation of only smart contract interactions for role verification and token-authenticated login verification.
- Fully Blockchain-Based Systems consume up to 80,000 gas units per user. This includes question presentation, answer submission, result verification, and logging-all on-chain.

#### 5.3.2. Interpretation

Gas efficiency has direct consequences on operational expense and the environmental footprint of blockchain solutions. Ethereum gas fees are dynamic, based on network congestion, and excessive gas usage incurs a higher cost per transaction, as well as longer confirmation times. DeCentralEx, by restricting interaction on the blockchain to verification, greatly reduces such problems, resulting in lower costs and latency. This is consistent with Research Objective 8: deploying a gas-efficient system suitable for real-world education implementations. By substituting less dependence on smart contracts for non-sensitive operations, DeCentralEx preserves the blockchain's openness and trust while reducing its computational and financial costs.

### 5.4. Overall Evaluation of DeCentralEx Architecture

Across all performance metrics and figures reported, the hybrid nature of DeCentralEx has illustrated systematic advantages.

**Table 2:** Objective-by achievement across systems

| Criterion | Standard Online | Encrypted Online | DeCentraEx(Hybrid) | Full Blockchain |
|---|---|---|---|---|
| Security Score | Low | Moderate | High | Very High |
| Tamper Resistance | Low | Moderate | High | Very High |
| Cost Efficiency | Very High | High | Moderate | Low |
| Scalability | Very High | High | Very High | Low |
| Gas Consumption | NA | NA | Low | High |

Table 2 illustrates the extent to which each test model satisfies the research objectives outlined in the methodology section. It is a verification tool throughout the verification process to check for consistency between the system's functionality and goals.

#### 5.4.1. Key Observations

- DeCentralEx meets all objectives mentioned, affirming its status as a complete and secure test framework.
- Encrypted and legacy systems fail to achieve objectives related to decentralization, transparency, and immutable logging.
- Full blockchain models meet most objectives but lack efficiency and practical scalability for deployment.

DeCentralEx implements a symmetric architecture, avoiding the traditional trade-offs between security, scalability, and cost. It uses smart contracts to handle only essential processes, such as user role validation, and delegates all other processes to a secure, encrypted off-chain solution. It thus provides a feasible and responsive framework for mass-scale academic testing.

#### 5.4.2. The Current Method Also Offers the Possibility of Further Extension into Some of the Following Areas

- Implementation with zero-knowledge proofs (ZKPs) for answer evaluation.
- On-chain hashing of exam logs to support integrity verification.
- Deployment onto L2 chains, such as Polygon, can further reduce the cost.

### 5.5. Alignment of Research Objectives

Upon reviewing the results,

- **They are Parallel to The Adjusted Research Objectives:** Strengthen the Confidentiality of Test Data: Achieved by storing test papers and final results off-chain, encrypted. Only the cryptographic reference is stored on a chain. The platform's design allows for approved MetaMask wallet owners to decrypt the data.

- **Reduce Blockchain Costs While Maintaining Security:** Exhibited through low utilization of on-chain data and brief transaction references. Comparison in Figures 8 and 10 indicates a lower gas overhead, as extensive exam material is stored off-chain, resulting in lower transaction fees per unit.
- **Enable Scalable Exam Processes:** Achieved by the ability of the system to support up to 15,000 examinees without performance decline, a result verified by load tests that utilize a distributed storage layer combined with on-chain proof-of-exam logs.
- **Keep Integrity and Tamper Resistance Simple:** Secured by an immutable record book of blockchain and hashed pointers for testing data. Any tampering will cause a mismatch in hashed records, hence tamper detection and data integrity assurance.
- **Create Secure User Identification with MetaMask:** Enabled by wallet login and smart contract verifications, it prevents unauthorized accounts from viewing or sending exam information. Smart contracts bind user behavior to autonomous wallet addresses, and impersonation is kept in check.
- **Avoid Single-Point Failures:** Governed by the consortium blockchain model, whereby several fair nodes take turns in maintaining the recordbook. Neither a small node breach nor a large one will cause the entire network to collapse, allowing exam processes to continue uninterrupted.
- **Enable Efficient Dispute Resolution:** Confronted with cryptographically assured timestamps for submission and ultimate scores. Administrators can ask a user about their on-chain transaction history, enhancing their capacity to make an equitable determination of grading disputes or second-submission requests.

### 5.6. Deployment Consequences and Limitations

While DeCentralEx is a strong solution, some limitations were observed:

- It relies on MetaMask or a similar Ethereum wallet for identity verification purposes.
- Network latency and the price of gas, though optimized, remain dependent on the underlying infrastructure of Ethereum.
- Current deployment on Sepolia Testnet is not indicative of a production-scale environment.

Nonetheless, these are technical, not architectural, limitations, and with migration to optimized L2 chains or with walletless authentication, the prospects for mass deployment of DeCentralEx are high.

## 6. Conclusion

This work introduces DeCentralEx, a decentralized and scalable testing platform designed to overcome the limitations of conventional and exclusive blockchain-based internet testing platforms. In combination with encrypted cloud storage and smart contract-based authentication, DeCentralEx introduces a secure, tamper-resistant, but economical hybrid framework that keeps the system scalable. The experiment demonstrated that decentralized authentication can efficiently prevent unauthorized access, while off-chain encrypted storage minimizes gas consumption and reduces operational costs. Performance evaluation indicated that DeCentralEx performs better than conventional online systems in terms of integrity and reliability and outperforms complete blockchain models in terms of scalability and affordability. Parameters like security score, tamper resistance, gas efficiency, and concurrent user capacity validate the feasibility of the system. Notably, DeCentralEx accommodates a maximum of 15,000 concurrent users with negligible blockchain overhead, presenting a trade-off solution for schools that demand secure, high-scale deployments.

Furthermore, the system achieves all necessary research goals, including secure role authentication, data privacy, time-limited testing, and automatic grading. AES encryption of questions and real-time smart contract authentication of user roles ensure that test data is kept private and tamper-free. Lastly, DeCentralEx is a functional, adaptable, and technically sound solution for conducting secure online examinations. As a hybrid solution, it demonstrates the potential to integrate decentralized technologies with conventional cloud services, aiming to address existing gaps in digital exam systems. Further research can be allocated for advanced cryptographic optimizations and L2 blockchain network deployment to optimize performance further and reduce transaction fees.

**Acknowledgment:** The authors express their sincere gratitude to SRM Institute of Science and Technology for the support and resources provided. They also acknowledge the encouragement and cooperation received throughout the course of this research.

**Data Availability Statement:** The data supporting the findings of this study are available from the corresponding authors upon reasonable request.

**Funding Statement:** This manuscript and research paper were prepared without any financial support or funding.

**Conflicts of Interest Statement:** The authors declare no conflicts of interest. This work represents a joint contribution by the authors, and all citations and references are appropriately included based on the information utilized.

**Ethics and Consent Statement:** This research adheres to the highest ethical standards, with informed consent obtained from all participants.

**References**

1. A. K. Samanta, B. B. Sarkar, and N. Chaki, "A blockchain-based smart contract towards developing secured university examination system," *Journal of Data, Information and Management*, vol. 3, no. 3, pp. 237–249, 2021.
2. Y. N. Patil, A. W. Kiwelekar, L. D. Netak, and S. B. Deosarkar, "A decentralized and autonomous model to administer university examinations," in Blockchain Technology for IoT Applications, *Springer*, Singapore, 2021.
3. A. Punia, P. Gulia, N. S. Gill, E. Ibeke, C. Iwendi, and P. K. Shukla, "A systematic review on blockchain-based access control systems in cloud environment," *Journal of Cloud Computing*, vol. 13, no. 146, pp. 1-37, 2024.
4. M. Abdelsalam, M. Shokry, and A. M. Idrees, "A proposed model for improving the reliability of online exam results using blockchain," *IEEE Access*, vol. 12, no. 8, pp. 7719–7733, 2024.
5. M. R. I. Sattar, M. T. B. H. Efty, T. S. Rafa, T. Das, M. S. Samad, A. Pathak, M. U. Khandaker, and M. H. Ullah, "An advanced and secure framework for conducting online examination using blockchain method," *Cyber Security and Applications*, vol. 1, no. 12, p. 100005, 2023.
6. C. V. N. U. B. Murthy, M. L. Shri, S. Kadry, and S. Lim, "Blockchain-based cloud computing: Architecture and research challenges," *IEEE Access*, vol. 8, no. 11, pp. 205190–205205, 2020.
7. M. S. Farooq, R. Tehseen, and U. Omer, "Blockchain based online examination assessment models for educational institutes: A systematic literature review," *VFAST Transactions on Software Engineering*, vol. 9, no. 3, pp. 57–67, 2021.
8. S. Kapse, M. Umalkar, A. Gajbe, K. Vrudhula, R. Gour, and S. Telrandhe, "Blockchain-based solution for secured transmission of examination paper," in *Proceedings of the 2022 IEEE 2nd International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, Odisha, India, 2022.
9. G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing," *Future Internet*, vol. 14, no. 11, p. 341, 2022.
10. W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, "Blockchain-based trust management in cloud computing systems: A taxonomy, review, and future directions," *Journal of Cloud Computing*, vol. 10, no. 35, pp. 1–34, 2021.
11. S. Song, "Construction of university online examination system based on cloud computing technology," *Scientific Programming*, vol. 2021, no. 12, pp. 1-12, 2021.
12. A. Singh, "Design, analysis and implementation of online competitive examination using heterogeneous consortium blockchain," *International Journal of Engineering and Technical Research*, vol. 10, no. 12, pp. 122-127, 2021.
13. M. A. Shinwan, A. Shdefat, N. Mostafa, A. A. Sokkar, T. Alsarhan, and D. Almajali, "Integrated cloud computing and blockchain systems: A review," *International Journal of Data and Network Science*, vol. 7, no. 12, pp. 941–956, 2023.
14. X. Zhu and C. Cao, "Secure online examination with biometric authentication and blockchain-based framework," *Mathematical Problems in Engineering*, vol. 2021, no. 1, pp. 1-12, 2021.
15. A. Jain, A. K. Tripathi, N. Chandra, and P. Chinnasamy, "Smart contract enabled online examination system based on blockchain network," in *Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2021.