IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 July 2023, accepted 3 August 2023, date of publication 14 August 2023,
date of current version 18 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3304995

RESEARCH ARTICLE

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

MOHAMED ABDELSALAM[1], MARWAN SHOKRY[2], AND AMIRA M. IDREES[3]
[1]Information Systems Department, Faculty of Commerce and Business Administration, Helwan University, Cairo 11795, Egypt
[2]Business Information Systems Program, Faculty of Commerce and Business Administration, Helwan University, Cairo 11795, Egypt
[3]Faculty of Computers and Information Technology, Future University in Egypt, New Cairo 11835, Egypt

Corresponding author: Marwan Shokry (marwanshokry_727@commerce.helwan.edu.eg)

ABSTRACT In recent times, Learning Management Systems (LMS) have gained significant popularity, particularly due to the COVID-19 pandemic, offering improved effectiveness and efficiency. Within LMS, online exams have emerged as a critical tool for assessing students' performance and understanding of course material, playing a vital role in determining their progression. Ensuring the reliability and transparency of online exam results is imperative. Any vulnerability, such as hacking, can adversely impact students' grades. Conventional online exam systems often store data centrally in databases like MySQL, making them susceptible to unauthorized access and manipulation. This paper presents a blockchain-based framework to enable secure and peer-to-peer conduction and evaluation of academic exams. The framework uses hashing techniques to ensure data integrity and employs proof of stake mechanisms for enhanced security. Blockchain's decentralized data storage and cryptographic hashing for each block make it effective in safeguarding data integrity. The paper demonstrates the use of blockchain for developing online exams, storing each question and answer directly on the blockchain. To achieve this, we have created a module that integrates with the Moodle learning management system. Through a comparative analysis with Moodle's default centralized storage, our module modifies the exam result storage, ensuring secure and tamper-proof data storage on the blockchain. By leveraging the blockchain, exam data is reliably secured, maintaining integrity, and resisting manipulation. Our results show that data stored on the blockchain is entirely accurate, with no discrepancies compared to Moodle's standard approach. The blockchain network provides a reliable and immutable platform, preventing unauthorized changes to student data. In conclusion, our blockchain-based framework offers a robust solution for enhancing the security and reliability of online exam results. By harnessing blockchain's decentralized and tamper-proof nature, we ensure data integrity and transparency, providing a more trustworthy assessment of academic performance.

INDEX TERMS Blockchain, online test, online examination systems, smart contracts, Ethereum, meta mask wallet, learning management systems, LMS, Moodle, centralized ledger database, CLD.

I. INTRODUCTION

The occurrence of COVID-19 has drastically changed education all over the world. Many schools and universities have started to adapt new techniques in learning by considering online education instead of pen and paper. E-learning is like a network-enabled transmission of knowledge by using electronic applications to process learning [1]. It emerges the normal work with paper and gives a variety of technologies to provide more benefits for the students. Through which students can take their lectures in form of videos or tutorials that can be watched by them using their personal computers or laptops anytime they want [2]. It improves classroom interaction by creating an environment where they actively participate in online tutorials to accomplish a work that has been given to them [2]. A lot of advantages come with E-learning to students like the courses of lectures that are available on demand so students can revise the course or complete the given tasks. Also, it helps fast or slow learners, decreases stress and it allows communication with

The associate editor coordinating the review of this manuscript and approving it for publication was Rahim Rahmani.

students and addresses their issues immediately through the E-learning systems [1]. They can also benefit from online exams for preliminary screening in a meaningful and productive way. E-exams offer further advantages as well. When compared to traditional printed paper tests, these electronic exams save faculty members time and effort, and students are safer because the latter take a lot of time and work to correct, extract the scores, and announce them to students. E-exams are regarded as one of the most significant e-learning tools for gauging success [3].

Various online exams are being conducted being user-friendly, and being on centralized servers which can develop many issues and security breaches. Attackers may commit cheating, hacking the data stored or deleting exam content for that. It must offer a solution for securing its reliability, here Blockchain comes into play to solve the security and reliability issues as everything will be stored in manner they cannot be manipulated with. We will use LMS Moodle; as it is one the most LMS all over the world that provides a lot of features like to allow teachers to make online lectures, make assignments for students and make exams for them. As well as it has an auto grading system to automatically correct exams and send the grades to students.

In this paper, we aim to conduct a thorough comparison between the traditional centralized and modern decentralized learning management systems. Furthermore, we will provide an in-depth demonstration of our proposed model, which focuses on transforming an exam into a web application. This model will facilitate the submission of exam answers and results directly onto the blockchain as a new block, along with an explanation of the process of transaction fee deduction from the user's wallet for submitting data to the blockchain. Our innovative model will allow students to log in, take their exams, and once completed, submit their answers directly onto the blockchain network. The exam administrator can then access a dashboard displaying all submitted answers.

The main contribution of the paper is the proposal of an innovative model that utilizes blockchain technology to transform exams into a web application. This model enables students to log in, take exams, and submit their answers directly onto the blockchain network. The proposed model offers several advantages. First, by leveraging blockchain technology, the model enhances security and reliability by storing exam data in a tamper-proof manner that cannot be easily manipulated. This address concerns cheating, hacking, and unauthorized alteration of exam content. Additionally, the model utilizes the LMS Moodle, a widely used learning management system, which provides various features such as online lectures, assignments, and exam creation. By integrating the proposed model with Moodle, it allows for seamless administration of exams within the familiar LMS environment. Furthermore, the model introduces an auto-grading system that automatically corrects exams and sends the grades to students. This streamlines the grading process and provides timely feedback to students.

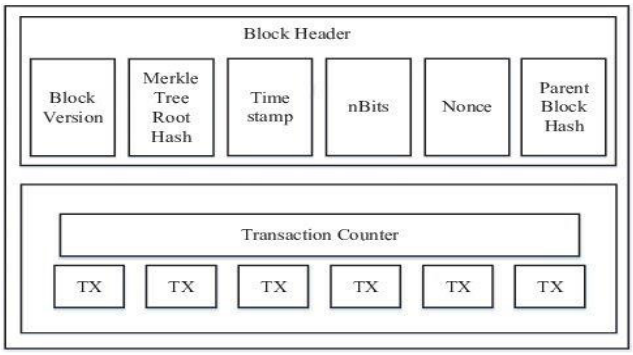

FIGURE 1. An overview of blocks in the blockchain [4].

In summary, this paper's primary contribution resides in introducing and showcasing an inventive model that integrates blockchain technology, the Moodle LMS, and an auto-grading system. The overarching goal is to elevate the security, reliability, and efficiency of online exams. By leveraging blockchain's immutability and transparency, the proposed model aims to address the challenges associated with centralized exam systems and provide a secure and reliable solution for conducting online exams.

II. BACKGROUND

A. BLOCKCHAIN

is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. With each transaction a block is created and stored to network then this chain will grow more and more. So, every block is being stored in decentralized way [4].

Figure 1 illustrates the block characteristics in blockchain network, every block contains header and body, each block header contains previous block hash to ensure the integrity. The block body contains the transaction counter and the transaction itself. Blockchain uses an asymmetric cryptography technique to ensure the authentication of transactions [4]. We will use blockchain technique to save our exam grades data.

B. SMART CONTRACT

is an application that operates on top of the blockchain. It is a block of code that can be run when specific requirements are met. Its goal is to make agreements between unreliable parties easier to follow through on and enforce them. It could be compared to a system that distributes digital assets to a number of interested parties if certain conditions are satisfied [6]. As compared to other traditional contracts, the operation of smart contracts is not dependent on the trusted third party and thus reduces the transactional cost. Smart contracts can be developed by utilizing different blockchain platforms, but the most common to use is Ethereum. It supports more features than other platforms and makes the creation and customization easier [5]. We can apply smart contracts to

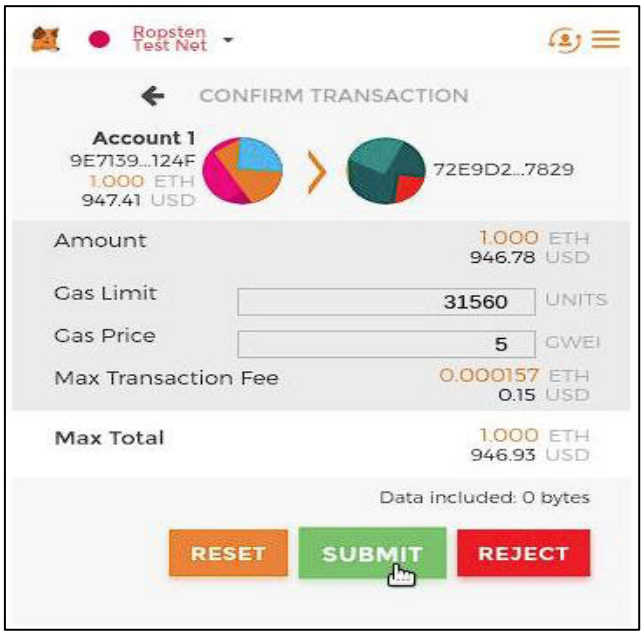

FIGURE 2. Sending 1 ether to the contract address [7].

learning management systems. Some of the main benefits of smart contracts are:

A. Speed, efficiency and accuracy: as the contract is automated, it is executed immediately as the condition is met without wasting time.
B. Savings: while using smart contracts, there is no need for third-party involvement, thus avoiding time delays and fee charges.
C. Security: all the transaction records in the blockchain.

We will use smart contracts to interact and submit students answers and grades to be saved in the blockchain network.

C. ETHEREUM

is a decentralized computing infrastructure that we can use to execute programs like smart contracts as it interacts with users to get the transactions they made or data they submit to blockchain network. Along with being used as cryptocurrency that are called ether, it allows developers to build decentralized apps on the top of blockchain to ensure availability, auditability, transparency, and neutrality [7].

Figure 2 illustrates the currency being sent to a specific address using either cryptocurrency and MetaMask wallet which we will explain during the research. We will use our model to build our smart contract that will help us to store data and its cryptocurrency ether to pay for the data to enter the blockchain network.

D. SOLIDITY

is an object-oriented programming language created specifically by Dr. Gavin Wood for constructing and designing smart contracts on Blockchain platforms. It's used to create smart contracts that implement business logic and generate a chain of transaction records in the blockchain system. It has a lot of similarities with C and C++ and is pretty simple to learn and understand. For example, a "main" in C is equivalent to a "contract" in solidity [7]. This is the programming language that will be used to code our smart contract, to publish it to students, to submit their answers then it will take their grades and be stored in the blockchain network.

E. MetaMask

is crypto currency wallet that is equipped with a key vault, secure login, its token wallet, and token exchange everything you need to manage your digital assets. We can use to pay by crypto currencies or if someone wants to receive crypto. It is a web browser extension or can be used as mobile app downloaded. The extension enters the Ethereum web3 API into website's JavaScript; so, the webapp could read data from Blockchain MetaMask also let the user create and manage their wallet. Then when users need to create any transaction it will pop-up with an interface so user can review transaction before paying any crypto as well as it requires user to enter their username and password every time the browser closes. We will use it here to get ID account on the Ethereum network, then check if the user belongs to this network or not and pay the crypto to submit answers to the network [8]. It will be used by the students as their crypto currency wallet that they will use to pay for the submission of their test to be stored in the blockchain network as well as it will ensure that there is an account id to pay for the submission.

F. MOODLE

is an open-source learning platform that is assigned for online learning, distance education, flipped classroom and projects in schools or universities [9]. It is a complete LMS that has classes and different dashboards for admins, teachers, and students. Online classes schedules as well as online exams are widely used in many schools and universities online teaching and learning, and it is used especially in STEM (science, technology, engineering and math) education [10]. We will illustrate our model based on this Webapp to show how our module works. It will be used to adapt our module to it. Nowadays, it is considered one of the most popular LMS that is being used by a lot of schools and universities.

G. GANACHE

is like a local or personal Ethereum environment that helps us to test or inspect states [11] as it gives us a bench of private keys that can generate address with it for enabling us to run tests. It allows us as well to check if there is a new block that has been added to blockchain and the amount of crypto taken form account per transaction. It will be used to have a similar situation like a local blockchain network to run our module test and make transactions to save data in blockchain network.

H. LEDGER DB

is a centralized ledger database (CLD) that provides tamper-evident, non-repudiable, and highly auditable features. It is similar to a blockchain in that it provides a tamper-evident and non-repudiable ledger, but it does not have the same decentralized architecture as a blockchain. It also offers stronger auditability than a blockchain by adopting a TSA two-way peg protocol. This protocol prevents malicious behaviors from both users and service providers, and it allows for verifiable data removals [12].

III. SECURITY OF ARCHITECTURE

In our research, we acknowledge that data security and privacy are crucial considerations when integrating the blockchain with the Moodle learning management system (LMS). We have implemented substantial measures to guarantee the confidentiality, integrity, and privacy of data and user information within the decentralized system.

To enhance data and user security, we have integrated the HTTPS protocol for data transmission between the website and the blockchain. HTTPS ensures a secure and encrypted channel for data communication, effectively safeguarding the information shared between users and the system. The adoption of HTTPS significantly mitigates risks such as eavesdropping, man-in-the-middle attacks, and unauthorized access.

Furthermore, we employ Web3.js, a widely embraced JavaScript library, to interface with the blockchain. Web3.js inherently incorporates robust encryption and cryptographic protocols, guaranteeing secure communication with the blockchain network. The utilization of Web3.js, coupled with HTTPS, introduces an additional layer of security to data transmission and interactions with the blockchain.

IV. RESEARCH CONTRIBUTION

Our research primarily centers around proposing and showcasing an inventive model that integrates blockchain technology, the Moodle LMS, and an auto-grading system. The aim is to elevate the security, dependability, and efficiency of online exams. Our objective is to demonstrate the feasibility and potential of this model in effectively tackling the challenges linked to centralized exam systems.

While we agree that thorough system benchmarking requires more robust methodologies and metrics, such as performance tests, scalability analysis, and comparative evaluations, we would like to clarify the purpose and scope of our research. The inclusion of desktop-generated screenshots serves to illustrate the user interface and workflow of the system, providing a visual representation of how students interact with the web application and submit their exam answers onto the blockchain network.

We acknowledge that desktop-generated screenshots alone may not be sufficient for conducting a comprehensive benchmarking analysis. However, as our primary emphasis is on the conceptual framework and practical implementation of the proposed model, we believe that the inclusion of these screenshots is appropriate to support the visualization of our innovative approach.

To further enhance the credibility and validity of our research, we plan to conduct future work that includes comprehensive system benchmarking using appropriate tools and methodologies. This will allow for a more in-depth analysis of the model's performance, scalability, and other relevant metrics.

Our main contribution lies in the development of an integrated model that combines blockchain technology, the LMS Moodle, and an auto-grading system to address the challenges associated with online exams. While individual components of our architecture may not introduce new concepts in data security, privacy, or performance, it is the unique combination and integration of these components that offers a novel solution to the problem at hand.

In terms of data security, our architecture leverages the immutability and transparency of blockchain technology to ensure the integrity and tamper-resistance of exam data. By storing exam data on the blockchain, we provide a secure and trustworthy environment that mitigates the risk of data manipulation or unauthorized access. While the use of blockchain for data security is not new, our application of it within the context of online exams, specifically integrated with the Moodle LMS, adds a novel dimension to the existing literature.

Regarding privacy, our architecture incorporates privacy-enhancing techniques such as data anonymization and access control mechanisms. These measures protect the sensitive information of students and ensure compliance with privacy regulations. While privacy-preserving techniques are not unique to our architecture, the integration of these techniques within the context of online exams, alongside blockchain and the Moodle LMS, presents a novel approach that balances data security, privacy, and performance.

Furthermore, the integration with Moodle LMS, a widely used learning management system, provides a seamless and familiar environment for conducting online exams. This integration enhances usability and user experience, addressing the performance aspect of our architecture. While the use of an LMS for online exams is not novel, our specific integration with Moodle, in combination with blockchain technology and the auto-grading system, adds a unique and innovative dimension to the existing literature.

Lastly, our model introduces an auto-grading system that automates the correction of exams and delivers timely grades to students. This automation streamlines the grading process, improves efficiency, and enhances the overall performance of the system. While auto-grading systems have been explored in various contexts, our integration of such a system within the proposed architecture, along with the other components, contributes to the novelty of our research.

In conclusion, while individual components of our architecture may not introduce new concepts in data security, privacy, or performance, the innovative aspect lies in the integration and combination of these components within the

context of online exams. By combining blockchain technology, the Moodle LMS, and an auto-grading system, our architecture provides a comprehensive solution that balances data security, privacy, and performance. We believe that the unique combination of these components and their integration into the online exam context demonstrates the novelty of our research.

V. LITERATURE REVIEW

A lot of researchers provide different perspectives to provide an appropriate approach for securing online exam results. In this section, we will discuss some of the approaches.

Jain et al. [13] had proposed a model for the e-learning platform in which student pay for the examination using crypto then solve the exam and then this data are saved as smart contract in the blockchain network, however they make the students enter their addresses and it is saved to the database that it can be tempered with by changing the address of student to another address so the student result can be not accurate.

Yuan et al. [14] have proposed a web based online examination system in which students can take their exams. Then the system will transmit the questions and results to the server then it will generate the grades for students. Shinde [15] have implemented a system for online exams with face detection to ensure students can't cheat during the exam and after the student finishes the exam the system can calculate marks and show the results. Rashad et al. [16] had proposed and built a web-based examination system that carries out the exams with various types of question like MCQs or essay questions, but it takes those to assess the difficulty of questions to evaluate. The system is intended to facilitate the conductance of exams with auto marking the submissions and issuance of a report about each exam taken. This system is built upon many web technologies like AJAX, PHP, HTML and MySQL database. It was also tested in Mansoura University in Egypt, and it proves its validity but the structure of this web-based examination system that it stores everything in centralized location in which all data are found in the data bank as in Figure 3.

Fagbola et al. [17] had proposed a webapp online exams to support the examination process and fix some of problem that exist in various webapps like automatically logging of the student upon expiration of allotted time. It is developed to address those problems that facilitate other aspects of the examination process like supporting auto-submission, auto marking and examination result report generation. likewise, it is also built upon front-end development of the web like HTML and Microsoft Visual Studio development environment with the use of SQL Server as the database of the webapp that will sane everything about the examination process. But as illustrated in Figure 4, every conducted process will be stored in centralized location but in all the previous systems, they have used a centralized database in which the data can be manipulated, so, this means that the results

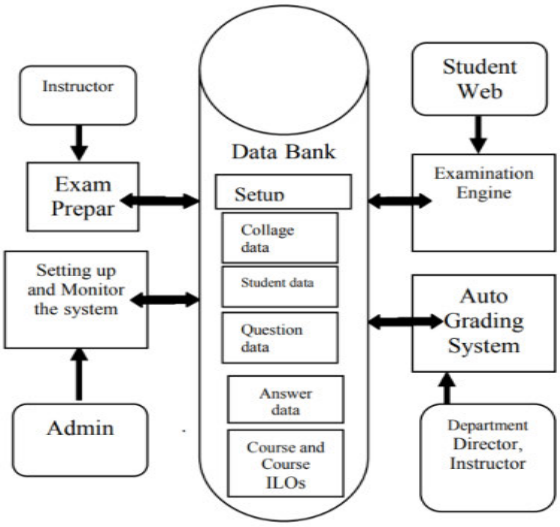

FIGURE 3. System architecture [15].

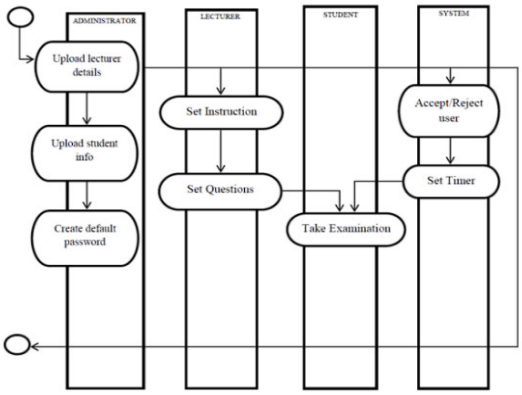

FIGURE 4. Diagram for the CBT (Computer-Based Test) system [16].

obtained from the system aren't reliable but blockchain here can solve this problem.

Rooksby and Dimitrov [18] had proposed a system based on Ethereum platform and Smart contract that helps to save student's course information and grades at the university of Glasgow. The grades stored to the blockchain network are transparent. The system proves to be highly trustworthy. They didn't provide a complete case study for their work to assess the validity of the system for ensuring the system outcomes as well as they didn't provide the system accuracy for saving student's grade in the blockchain.

Pee et al. [19] had they designed online testing system based on blockchain and CP-ABE encryption in which the system admin provides specific teacher for every test being taken to set the questions by using their private key this to restrict access authority using CP-ABE algorithm. Students can enter their exam and after saving their scores in the blockchain for ensuring their integrity and they are not

manipulated. This system protects the exams scores and is characterized by its higher security.

The last two systems are designed for online testing based on blockchain for security. Our contribution is represented in that our module will be applied on Moodle that it is a complete LMS which provides all features needed for any online institution.

Yang et al. [20] proposed a new verification framework designed specifically for centralized ledger databases (CLD). This framework aims to achieve two essential goals: robust external auditability and rapid verification. The core concept behind this framework is known as Dasein verification, which combines the elements of what, when, and who validation to establish a formalized approach to ledger auditing. Additionally, they provide an overview of the system structure employed in the proposed framework, along with the findings from its performance evaluation. The evaluation results indicate that the framework demonstrates a remarkable 23-fold increase in verification throughput and a significant 500-fold reduction in latency when compared to Hyperledger Fabric in notarization applications. Then to solve the issue for the CLD regarding the timestamp as the time of a transaction is important because it can be used to determine its authenticity and validity. For example, if a transaction is claimed to have been made at a certain time, but the time verification shows that it was made at a different time, then the transaction may be fraudulent. LedgerDB can solve it based on the paper It proposes a two-way timestamp pegging protocol. In which both the digests of data and the actual data are submitted to the trusted third party. This means that the attacker cannot tamper with the data without also tampering with the digests of data. As CLD that provide verifiable timestamps, uses one-way timestamp pegging protocol that can arouse infinite time amplification problem. LedgerDB solves the problem of securing the data in a manner that is difficult to be tempered by a hacker or attacker. But in our case here, we needed the blockchain network itself, as based on our proposed model, we use a private blockchain network to verify the student first if it belongs to the university by using his private key, with which he can take the exam. Then we use a smart contract to save his data to the blockchain network, where it will be secured.

Nowadays, online exams and quizzes are very important in any learning management system, but it is important to obtain results with high reliability, accuracy and tamperproof from LMS. However, the problem is that most of them are using centralized databases which are not the best ways to store results as anyone can access the database and change records.

In Figure 5, we have developed a generic module to use it in any examination platform, and we apply it on the Moodle LMS as it is one of the best open sources LMS in this field of online education as it allow to use to make different profiles for admins, teachers and students as well as allow to give them certain privileges. It also allows students to lay the syllabus and categorize them then allow certain students to take those courses. It allows students to check their schedule for the courses they take. It allows the teachers to submit exams to students this where our module will take place as answers submitted by student are stored in centralized database which it is MYSQL database that it can be tempered by hackers and this will reflect the student grades and data become inaccurate and can't be used as authentic data as it does not reflect the correct grades for student.

VI. OBJECTIVE AND SOLUTIONS

We have developed our module with blockchain to save online exams answers that are submitted by students as if answers being submitted and exam grade will be saved as block in the blockchain network that is mainly impossible to be hacked or tempered by anyone as Blockchain is immutable which means that it is a permanent and unalterable network, decentralized which there is no central place that saves the data like MYSQL.

Then after student's log in to the system they will be prompted to start their exam after the system checks the validity of their account id and the wallet connected to an account. After that they can take the exam and submit their answers using the MetaMask wallet to pay for the submission of their exam. As we are going further through research paper, we will illustrate our proposed model in Figure 6, in which illustrates the working of this webapp, the first step is login which it will be handles by Moodle. The student will fill out his information like username and password where they are stored in MYSQL database the app will check the username and password, then the students will go to the exam page where they will be asked to import their account to wallet if they didn't do that already then app will check the validity of their private key this is handled by MetaMask Ethereum blockchain wallet then check the validity of the address if it belongs to the college network.

After that the exam will be presented to the students to answer it, after answering the exam the students will be asked to confirm the transaction for submitting their answers to blockchain network, which is done by MetaMask Ethereum blockchain wallet, after transaction is confirmed then student's answers will be stored as block in the blockchain network which will be secured and can't be tempered with. Finally, the admin can now open dashboard to specify the students who have submitted the exam and their results which will come from the blockchain network.

VII. EXPERIMENTAL SETUP DESCRIPTION

In Figure 7, first we will build our smart contract using solidity programming languages and Ethereum along with truffle JS to generate our Json file for the contract that will used in Moodle to allow students to submit their questions answers and grades to be saved in the blockchain.

Algorithm in figure 7: Adding a student

1: Start

2: Declare a struct named "Student" with the fields:

- studentId (uint)
- name (string)

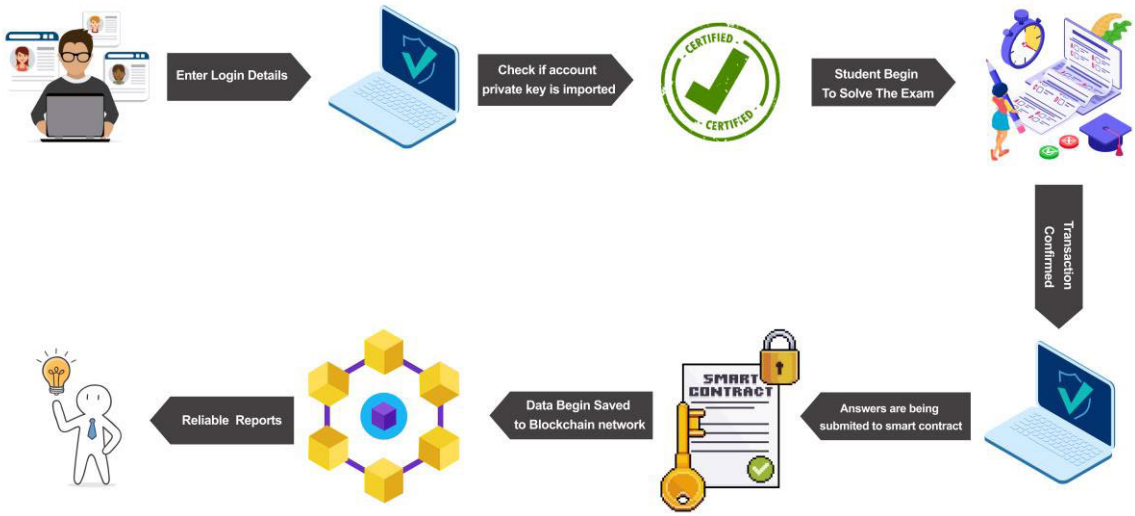

FIGURE 5. Structure of proposed model.

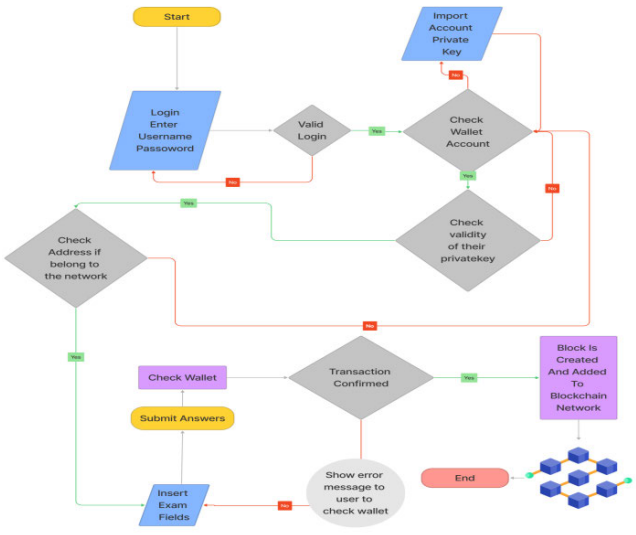

FIGURE 6. Our Blockchain Learning Management System (BLMS) proposed structure.

```
contracts > Exams.sol
contract Exam {
    // Modal Exam
    struct Student {
        uint256 studentId;
        string name;
        uint256 firstQuestion;
        uint256 secondQuestion;
        uint256 thirdQuestion;
        uint256 fourthQuestion;
        uint256 fifthQuestion;
        string completeDate;
        string timeTaken;
        string grade;
    }

    //fetch student with accountId
    mapping(uint256 => Student) public students;

    //store accounts that have submited exams
    mapping(address => bool) public alreadySumitedStudents;

    //Store Candidate Count
    uint256 public studentCount;

    //Constructor
    constructor() public {
```

FIGURE 7. Smart contract 1.

- firstQuestion (uint)
- secondQuestion (uint)
- thirdQuestion (uint)
- fourthQuestion (uint)
- fifthQuestion (uint)
- sixthQuestion (uint)
- finalResult (uint)
- grade (string)

3: Declare a mapping named ‘‘students’’ that maps a uint to a student struct.

4: Declare a mapping named ‘‘alreadySumitedStudents’’ that maps an address to a bool value that is used to view if student submitted before or not and view an error message if the student already submit.

5: Declare a uint variable named ‘‘studentCount’’ and initialize it to 0.

6: Define a function named ‘‘addStudent’’ that takes the following parameters:

- studentId (uint)
- name (string)
- firstQuestion (uint)
- secondQuestion (uint)
- thirdQuestion (uint)
- fourthQuestion (uint)
- fifthQuestion (uint)
- sixthQuestion (uint)

FIGURE 8. Smart contract Json file.

- finalResult (uint)
- grade (string)

7: Check if the student has not already submitted an exam: - Use the require statement to check if the boolean value at alreadySumitedStudents[msg.sender] is false.

8: Set alreadySumitedStudents[msg.sender] to true to mark the student as having submitted the exam.

9: Increment the studentCount variable by 1.

10: Create a new Student struct and assign it to students[studentCount]:

- Set the studentId field to the value of the studentId parameter.
- Set the name field to the value of the name parameter.
- Set the firstQuestion field to the value of the firstQuestion parameter.
- Set the secondQuestion field to the value of the secondQuestion parameter.
- Set the thirdQuestion field to the value of the thirdQuestion parameter.
- Set the fourthQuestion field to the value of the fourthQuestion parameter.
- Set the fifthQuestion field to the value of the fifthQuestion parameter.
- Set the sixthQuestion field to the value of the sixthQuestion parameter.
- Set the finalResult field to the value of the finalResult parameter.
- Set the grade field to the value of the grade parameter.

11: End

This is the process of adding a student and their exam details to a Solidity smart contract.

In Figure 8, we provide an example of a JSON file that will be utilized in Moodle to facilitate the submission of answers

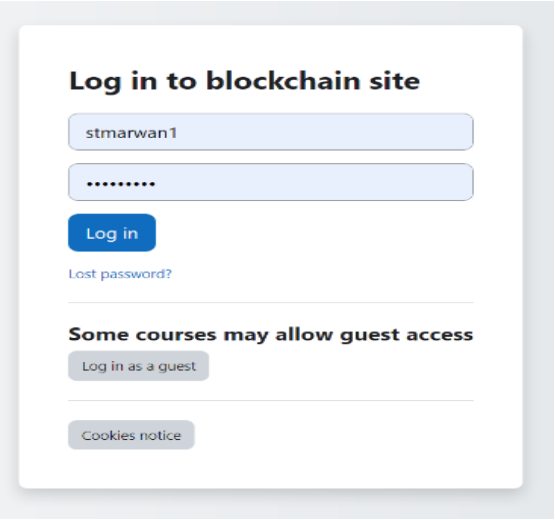

FIGURE 9. Login screen.

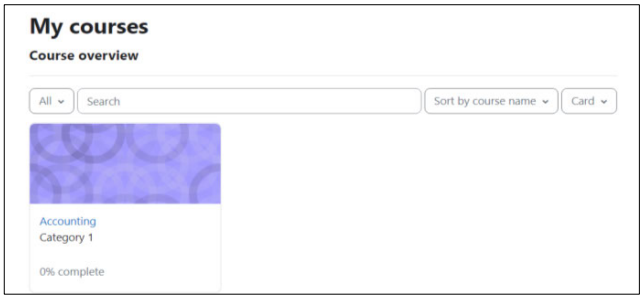

FIGURE 10. Student courses.

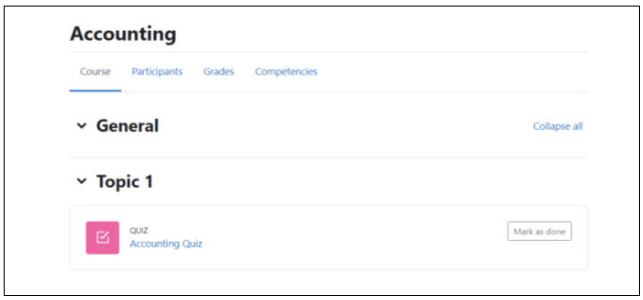

FIGURE 11. Student quizzes.

to the smart contract. This JSON file serves as a mechanism for interacting with the smart contract system. Now, let's delve into the exam process itself, including the display of error messages and the authentication of user accounts.

During the exam process, students will navigate through the assessment interface, where they can view and answer the exam questions. If any errors or issues occur, appropriate error messages will be displayed to guide students in resolving them. These error messages aim to provide clarity and assistance throughout the examination.

In Figure 9, we utilize the login screen provided by Moodle, enabling students to access the Learning Management

```
// Check if there is any private key imported to metamask or not.
if (err === null && account !== null) {

// Check if the account id associated with private key are belong to the netwok or not.
  if(webVerifyAddress.eth.accounts.includes(account)){
  App.account = account;
  console.log("Your Account: " + account);
}else{
  Swal.fire({
    text: 'Invalid Private Key Please Use the one specified by the college then Refresh',
    icon: 'warning',
    confirmButtonText: 'Refresh',
  }).then(() => {
    location.reload(true);
  })
}
}else{
  Swal.fire({
    text: 'Please Import The Account Private Key To Meta Mask then Refresh',
    icon: 'warning',
    confirmButtonText: 'Refresh',
  }).then(() => {
    location.reload(true);
  })
}
```

FIGURE 12. The code of error message to enter account private key.

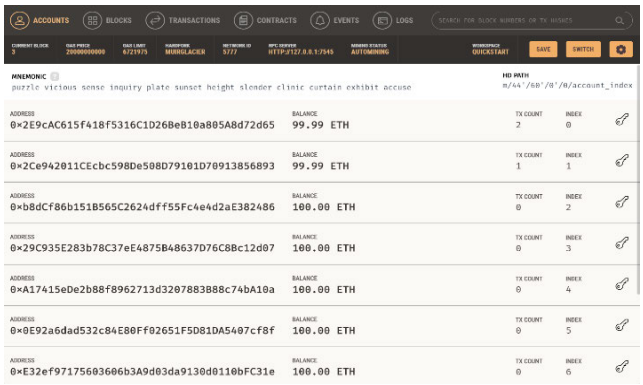

FIGURE 13. Get generated account private key.

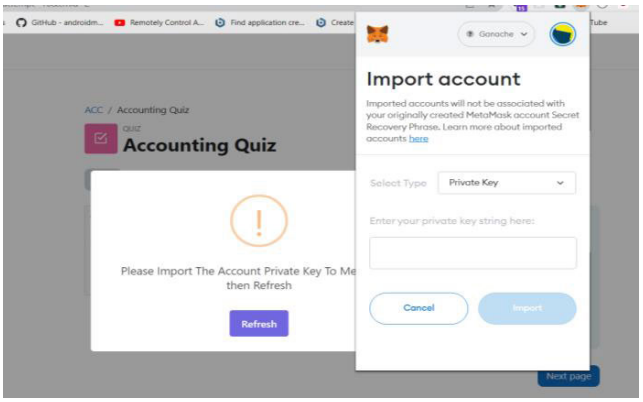

FIGURE 14. Importing private key to MetaMask.

System (LMS). The login information entered by students is subsequently stored in the Moodle database. This database serves as a repository for students to access their courses and any other resources offered by their respective educational institutions

In Figure 10, students will have visibility of all the courses they are enrolled in within the Moodle LMS. They can access the specific course they wish to engage with, which includes an associated exam that they need to complete. The exam process begins after passing various authentication steps, ensuring the secure commencement of the examination.

In Figure 11, after selecting a course, students will be directed to another screen where they can choose the specific quiz they wish to complete. This screen provides options and allows students to select the quiz that aligns with their intended examination.

In Figure 12, the examination is facilitated through the Moodle examination module. When a student enters the exam, the system verifies whether the student has entered their account's private key in MetaMask. If the private key has not been entered, the system will generate an error message requesting the student to input their private key, which is provided by the school or college. This error message appears as a popup notification to notify and guide the student in successfully accessing the exam.

In Figure 13, we utilize Ganache to obtain the private key that will be used in our example to illustrate how students can import their private key into MetaMask. This process enables

```
// Check if there is any private key imported to metamask or not.
if (err === null && account !== null) {

// Check if the account id associated with private key are belong to the netwok or not.
  if(webVerifyAddress.eth.accounts.includes(account)){
  App.account = account;
  console.log("Your Account: " + account);
}else{
  Swal.fire({
    text: 'Invalid Private Key Please Use the one specified by the college then Refresh',
    icon: 'warning',
    confirmButtonText: 'Refresh',
  }).then(() => {
    location.reload(true);
  })
}
}else{
  Swal.fire({
    text: 'Please Import The Account Private Key To Meta Mask then Refresh',
    icon: 'warning',
    confirmButtonText: 'Refresh',
  }).then(() => {
    location.reload(true);
  })
}
```

FIGURE 15. Checking if private key belongs to this network.

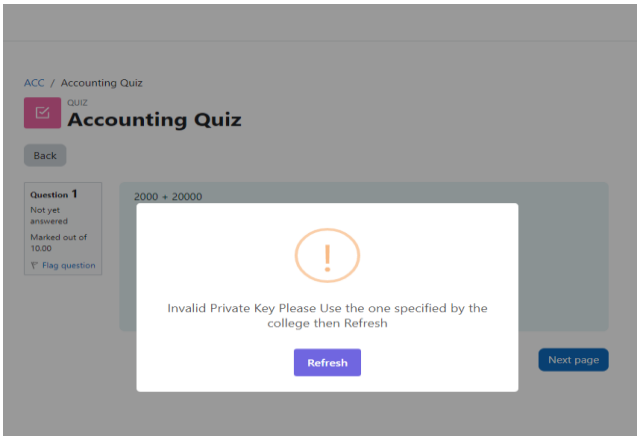

FIGURE 16. Error message to enter account private key in frontend.

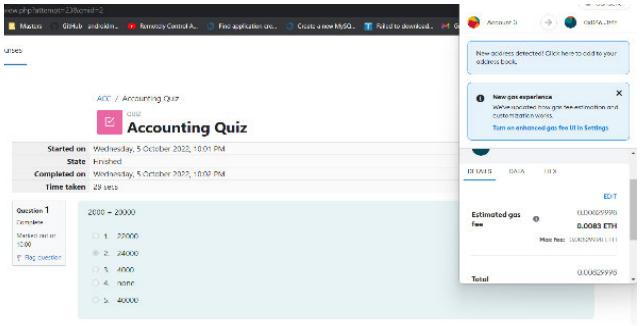

FIGURE 17. Confirm payment for exam.

students to access and participate in the exam. Following this, the system verifies whether the student's account ID, which can be obtained from the private key, is within the college or school network. This verification ensures that only authorized students from the respective educational institution can proceed with the exam.

In Figure 14, students will import their private key, which is provided by the college, to authenticate their affiliation with the specific college network. This authentication step ensures that the student is a valid member of the college's network and prevents unauthorized access from students belonging to other colleges or universities. By importing the private key, students establish their identity and eligibility to participate in the exam within the intended college network.

In Figure 15, the system retrieves the private key that the student has imported. Subsequently, it obtains the account IDs within the college or university network. Using the imported private key, the system generates the student's account ID. It then proceeds to verify whether this account ID belongs to the network by checking its existence within the network database. This step ensures that the account ID provided by the student is valid and authorized within the specific college or university network.

If the account ID does not belong to the network, an error popup message, like the one shown in Figure 16, will be

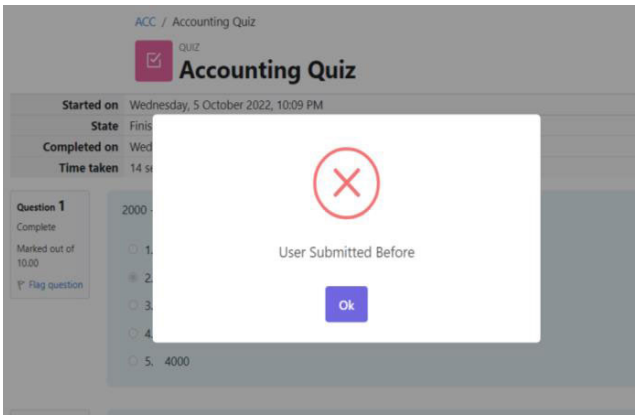

FIGURE 18. Error message show up if user submits again.

displayed to the student, prompting them to import the private key provided by the college. Importantly, this entire process takes place without storing the account ID or private key in a centralized database where they can be potentially accessed or manipulated. By avoiding centralized storage, the system ensures the security and integrity of the student's personal information and authentication details.

Once the student has completed all the exam questions, a popup will appear, seeking the student's permission to initiate a cryptographic transaction. This transaction aims to securely store the student's answers on the blockchain network. The transaction process is facilitated through the MetaMask Ethereum Wallet, as illustrated in Figure 17.

Upon successful completion of the transaction, a hash is generated, serving as proof of the student's transaction on the blockchain. In the event of a failed transaction where a block hash is not generated, the corresponding cryptocurrency amount will not be deducted, and an error message will be displayed to the student.

It's important to note that the transaction amount is only deducted when both the transaction and data blocks are fully generated and verified. This ensures that the data is securely and accurately submitted to the smart contract and saved as a block in the blockchain network. The decentralized nature of the blockchain network makes it highly resistant to modifications or hacking attempts, thus ensuring the integrity and immutability of the submitted data.

Once the transaction has been successfully added as a block in the blockchain network, if the student attempts to resubmit the exam answers through any means, MetaMask will prevent any further transactions and display an error. If the student confirms their intention to proceed with the submission despite this error, a popup message will appear, indicating that the user has already submitted their answers, like the example shown in Figure 18. This prevents duplicate submissions and ensures that each student's exam answers are recorded accurately and only once within the blockchain network.

If the student attempts to submit their answers again after the transaction has already been successfully added to the blockchain, a new block will not be generated, and the answers will not be updated or added for that student. To prevent unauthorized submissions, the student's account ID is flagged, indicating that they have already submitted their answers. This flagging process ensures that the student cannot submit their answers again.

Figure 19 illustrates how the student's account ID is marked as "submitted," indicating that the answers have already been recorded and cannot be resubmitted. All of this data is authenticated and securely saved in the blockchain network, making it tamper-resistant. This ensures that no one can falsely flag the student's account and enables the system to maintain the integrity of the examination process.

VIII. CASE STUDY

We executed a case study involving 30 students enrolled in the Business Information Systems (BIS) program at Helwan University's College of Commerce and Business Administration in Cairo, Egypt. The study centered on the Internet Application (IA) exam for the academic year. To safeguard the security of online exam results, we seamlessly integrated our module into the Moodle Learning Management System (LMS).

Each student received a unique username, password, and private key from the college. The private key was required for submitting answers to the blockchain network. The exam process began with students logging into the Moodle LMS and selecting the course for the exam. If a student forgot to enter their private key into the MetaMask wallet before starting the exam, the system detected this and displayed a popup message prompting them to insert their private key.

We encountered another issue where some students attempted to use private keys obtained from the internet or other departments within the university. However, the system verified every private key, extracting the student's account ID and checking if it belonged to the college network. If the account ID did not match the college network, an error popup message was shown, directing the students to insert the private key provided by their college.

Once the students began the exam, they answered the questions presented randomly, utilizing the features available in the Moodle LMS. After completing all the questions, the students submitted their answers to the blockchain network, where their answers and grades were securely stored. Some students attempted to submit their answers multiple times after taking the exam, but the system rejected these subsequent submissions. Each time a student made a submission, a flag was placed on their account ID, preventing duplicate submissions. As a result, their wallet transactions failed, and an error message was displayed to them.

Upon successful submission of their answers to the blockchain network, a new block containing the student's exam final result and their answers was created and added

```
contracts > Exams.sol
41          uint256 fifthQuestion,
42          string memory timeTaken,
43          string memory completeDate,
44          string memory grade
45      ) public {
46          // require that they haven't Submited before
47          require(!alreadySumitedStudents[msg.sender], "User Submitted Before");
48
49          //record the one who submitted
50          alreadySumitedStudents[msg.sender] = true;
51
52          studentCount++;
53          students[studentCount] = Student(
54              studentId,
55              name,
56              firstQuestion,
57              secondQuestion,
58              thirdQuestion,
59              fourthQuestion,
60              fifthQuestion,
61              timeTaken,
62              completeDate,
63              grade
64          );
65      }
66  }
```

FIGURE 19. How error message appears show up if user submits again.

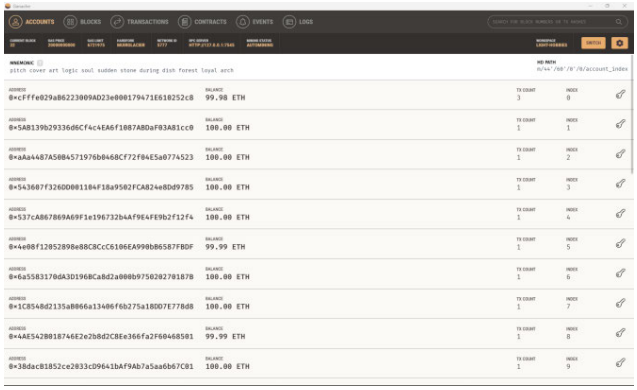

FIGURE 20. New block being added after submitting the data.

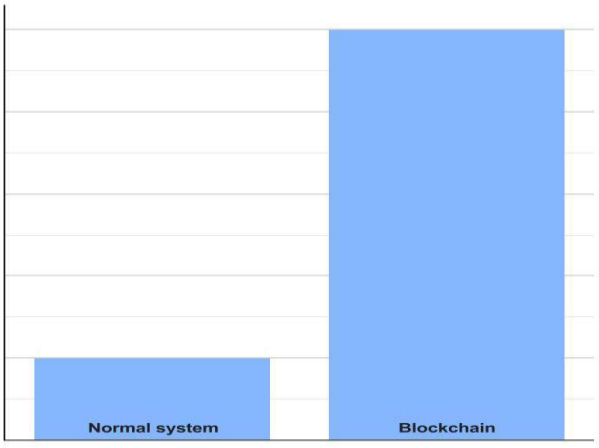

FIGURE 21. Level of transparency.

to the blockchain network. This block and its details can be viewed through Ganache, as shown in Figure 20.

Once the students have submitted their exam answers to the blockchain network, administrators can log in to a specially designed dashboard to access the students' exam results. This dashboard directly retrieves the results from the blockchain network, as depicted in Table 1. The utilization of blockchain in storing examination data has demonstrated successful implementation in this case study, ensuring transparency and accuracy. This approach was seamlessly integrated with one of the most renowned Learning Management Systems (LMS).

The conducted exam in our case study exemplifies the reliability and transparency of storing data on the blockchain network. Throughout the study, the data remained 100 percent accurate, with no instances of data loss. The system proved to be highly reliable and secure, effectively safeguarding against unauthorized access and manipulation.

TABLE 1. Admin dashboard to show students data from blockchain.

Student ID	Student Name	First Question	Second Question	Third Question	Fourth Question	Fifth Question	Complete Date	Time Taken	Student Grade
141558	Marwan Mohsen	2	0	0	0	2	Saturday, 19 November 2022, 9:13 PM	16 secs	33.33%
141559	Abdullh Ashraf	0	0	0	0	0	Saturday, 19 November 2022, 9:27 PM	1 min 13 secs	0%
141560	Tamara Emad	0	5	0	0	2	Saturday, 19 November 2022, 9:40 PM	13 secs	50%
141561	Afaaf Mohamed	0	5	0	0	2	Saturday, 19 November 2022, 9:40 PM	13 secs	50%
141562	Ameera Essam	0	5	0	0	2	Saturday, 19 November 2022, 9:40 PM	13 secs	50%
141563	Azmi Ashraf	0	5	0	2	2	Saturday, 19 November 2022, 9:13 PM	29 secs	66.66%
141564	Hossam el Badri	0	5	0	0	2	Saturday, 19 November 2022, 9:13 PM	43 secs	50%
141565	Saif Mohamed	0	5	0	0	2	Saturday, 19 November 2022, 9:13 PM	14 secs	50%
141566	Ahmed Ramadan	0	5	0	2	2	Saturday, 19 November 2022, 9:13 PM	29 secs	66.66%
141567	Farida Anwer	2	0	0	0	2	Saturday, 19 November 2022, 9:13 PM	16 secs	33.33%
141568	Maha Al-Basha	2	0	0	0	2	Saturday, 19 November 2022, 9:13 PM	16 secs	33.33%
141569	Mona El-Sayed	0	5	0	2	2	Saturday, 19 November 2022, 9:13 PM	29 secs	66.66%
141570	Mohamed Abdelhamid	2	0	0	0	2	Saturday, 19 November 2022, 9:13 PM	16 secs	33.33%
141571	Dalia Ahmed	2	0	0	0	2	Saturday, 19 November 2022, 9:13 PM	16 secs	33.33%
141572	Omar Ashraf	2	0	0	0	2	Saturday, 19 November 2022, 9:13 PM	16 secs	33.33%
141573	Nada Abd El-fatah	0	5	0	2	2	Saturday, 19 November 2022, 9:13 PM	29 secs	66.66%
141574	Ahmed Saber	0	5	0	2	2	Saturday, 19 November 2022, 9:13 PM	29 secs	66.66%
141575	Nabeela Abd El-wahab	0	5	0	0	2	Saturday, 19 November 2022, 9:40 PM	13 secs	50%
141576	Nada Fathy	0	5	0	0	2	Saturday, 19 November 2022, 9:40 PM	13 secs	50%
141577	Essam Ashraf	0	5	0	2	2	Saturday, 19 November 2022, 9:13 PM	29 secs	66.66%
141578	Nawaal Mohamed	0	5	0	2	2	Saturday, 19 November 2022, 9:13 PM	29 secs	66.66%
141579	Malk Ahmed	0	5	0	2	2	Saturday, 19 November 2022, 9:13 PM	29 secs	66.66%
141580	Ragab Attallah	0	5	0	2	2	Saturday, 19 November 2022, 9:13 PM	29 secs	66.66%
141581	Mohamed Abd El-rhaman	0	5	0	2	2	Saturday, 19 November 2022, 9:13 PM	29 secs	66.66%
141582	Saleem Ashraf	0	5	0	0	2	Saturday, 19 November 2022, 9:13 PM	14 secs	50%
141583	Salwa Nagi	0	5	0	0	2	Saturday, 19 November 2022, 9:13 PM	14 secs	50%
141584	Ashraf Mohamed	0	5	0	0	2	Saturday, 19 November 2022, 9:40 PM	13 secs	50%
141585	Shaden Mohamed	0	5	0	0	2	Saturday, 19 November 2022, 9:40 PM	13 secs	50%
141586	Aliaa Shosha	0	5	0	0	2	Saturday, 19 November 2022, 9:40 PM	13 secs	50%
141587	Yusri Mohamed	0	5	0	0	2	Saturday, 19 November 2022, 9:40 PM	13 secs	50%

This paper establishes that adopting blockchain technology for storing examination data can offer a trustworthy and secure solution, enhancing the integrity and transparency of the assessment process. By leveraging the capabilities of a well-established LMS and incorporating blockchain technology, the case study successfully demonstrates the potential benefits of this approach in the context of academic examinations.

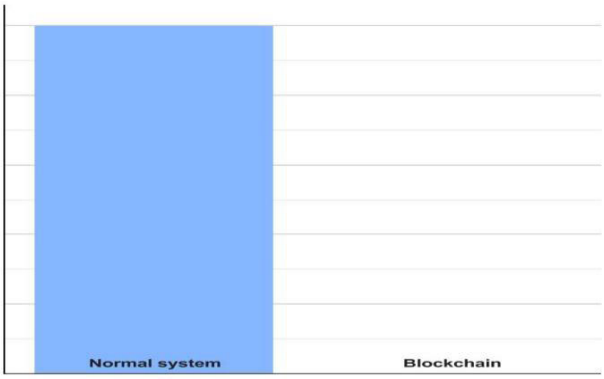

FIGURE 22. Chance of failure.

After conducting our case study, we proceeded to compare the performance of the system before and after implementing blockchain security measures.

In the traditional system without blockchain, the storage and management of examination data relied on centralized databases or servers. This approach often introduced vulnerabilities, such as potential data loss, unauthorized access, or manipulation. The system's reliance on centralized authority also limited transparency and made it difficult to ensure the integrity of the examination process.

In contrast, after implementing blockchain technology to secure the system, we observed several notable improvements. First and foremost, the decentralized nature of the blockchain network provided enhanced security and eliminated the risk of a single point of failure. The use of cryptographic techniques ensured the immutability of data stored on the blockchain, making it virtually tamper-proof.

The transparency of the blockchain network allowed for increased accountability and trust in the examination process. Each transaction and block on the blockchain could be independently verified, providing an audit trail of all student submissions and results. This transparency also minimized the potential for fraud or manipulation.

Furthermore, the integration of the blockchain with the existing Learning Management System (LMS) provided a seamless user experience. Students could securely submit their answers to the blockchain network, ensuring the authenticity and integrity of their submissions. Admins could easily access the exam results through a dedicated dashboard that directly retrieved data from the blockchain network.

Altogether, our comparison between the conventional system and the blockchain-secured system underscored the myriad advantages of integrating blockchain technology into examination data management. The blockchain approach offered enhanced security, transparency, reliability, and defense against unauthorized access or manipulation. These findings aptly illustrate the transformative potential of blockchain in reshaping the storage and management of examination data, ultimately elevating the entirety of the examination process.

IX. LEVEL OF TRANSPARENCY

Through our observations, we've discerned that our proposed system surpasses the conventional Moodle setup in terms of transparency. This enhancement is primarily owed to the encryption techniques harnessed by blockchain technology and the inherent decentralization of the system. Illustrated in Figure 21, our system's resilience stands as a formidable deterrent against data manipulation.

X. PROBABILITY OF FAILURE

Utilizing the blockchain network substantially decreases the likelihood of data loss, unavailability, or removal. This outcome stems from the intrinsic attributes of blockchain technology, where data is dispersed across numerous nodes. Consequently, the potential for failure is nearly eradicated compared to centralized databases. Each node within the blockchain network holds a copy of the data, ensuring its constant availability and resilience.

In contrast, centralized databases are susceptible to data removal or corruption by malicious actors. A single point of failure can result in data loss or integrity breaches. In contrast, the decentralized and distributed structure of the blockchain network ensures the security and safeguarding of data.

Integrating blockchain technology into the Moodle eLearning system offers a substantial enhancement in data security and reliability. Through the implementation of cryptographic techniques, blockchain guarantees a high level of trust in data protection. Visualized in Figure 22, the exceptional advantages that blockchain brings to reinforcing data security and maintaining data integrity within the Moodle eLearning system are evident. Notably, the integration of blockchain significantly diminishes the risk of failures, establishing a sturdy and enduring foundation for data management.

Overall, the incorporation of blockchain within the Moodle eLearning system substantially alleviates the perils linked to data loss, unavailability, and unauthorized tampering. It establishes a sturdy and durable structure that amplifies data security and reliability, thereby yielding advantages to the entire eLearning ecosystem.

XI. CONCLUSION

Our model centers around harnessing the blockchain network for the secure storage of exam results and grades. We juxtaposed this approach with Moodle LMS's default decentralized storage mechanism, augmenting it with the capabilities of blockchain technology. Through this integration, we guarantee the accessibility of transparent and dependable data. This data can be readily utilized by universities, colleges, and other institutions to confidently verify the precision of exam results.

In our implementation, we opted for the Ethereum platform to craft smart contracts that streamline the retrieval and storage of student data within the blockchain network. To create and validate our contract, we employed a robust programming language before seamlessly integrating it into Moodle. During the testing phase, we utilized Ganache to

obtain Ether currency, which enabled students to submit their answers onto the blockchain network.

Our case study showcased notable success in effectively securing and reliably storing data transferred from the LMS to the blockchain network. This achievement offers compelling evidence that blockchain stands as an ideal solution for augmenting the security and dependability of exam results.

Through the utilization of blockchain technology, we guarantee the integrity and transparency of exam data, creating a credible and unchangeable record of student performance. This approach presents a resilient solution to the data security and reliability challenges associated with exam results.

REFERENCES

[1] S. S. Gautam and M. K. Tiwari, "Components and benefits of e-learning system," *Int. Res. J. Comput. Sci.*, vol. 3, no. 1, pp. 14–17, Jan. 2016.

[2] A. Z. Al Rawashdeh, E. Y. Mohammed, A. R. Al Arab, M. Alara, B. Al-Rawashdeh, and B. Al-Rawashdeh, "Advantages and disadvantages of using e-learning in university education: Analyzing students' perspectives," *Electron. J. e-Learning*, vol. 19, no. 3, pp. 107–117, May 2021, doi: 10.34190/ejel.19.3.2168.

[3] M. E. Eltahir, N. R. Alsalhi, and S. S. Al-Qatawneh, "Implementation of E-exams during the COVID-19 pandemic: A quantitative study in higher education," *PLoS ONE*, vol. 17, no. 5, May 2022, Art. no. e0266940, doi: 10.1371/journal.pone.0266940.

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.

[5] A. Rosic. (2017). Smart Contracts: The Blockchain Technology That Will Replace Lawyers. Blockgeeks, Italy. Accessed: Apr. 3, 2023. [Online]. Available: https://blockgeeks.com/guides/smart-contracts/

[6] V. Buterin. *A Next-Generation Smart Contract and Decentralized Application Platform*. Accessed: Feb. 19, 2017. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper/

[7] A. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and DApps*. Sebastopol, CA, USA: O'Reilly Media, 2018.

[8] *Metamask*. Accessed: Jan. 20, 2023. [Online]. Available: https://metamask.io/

[9] *Moodle—Open-Source Learning Platform | Moodle.org*. Accessed: Feb. 19, 2022. [Online]. Available: https://moodle.org

[10] S. H. P. W. Gamage, J. R. Ayres, and M. B. Behrend, "A systematic review on trends in using moodle for teaching and learning," *Int. J. Stem Educ.*, vol. 9, no. 1, p. 9, Dec. 2022.

[11] A. Jabbar and S. Dani, "Investigating the link between transaction and computational costs in a blockchain environment," *Int. J. Prod. Res.*, vol. 58, no. 11, pp. 3423–3436, Jun. 2020.

[12] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, "LedgerDB," *Proc. VLDB Endowment*, vol. 13, no. 12, pp. 3138–3151, Aug. 2020, doi: 10.14778/3415478.3415540.

[13] A. Jain, A. Kumar Tripathi, N. Chandra, and P. Chinnasamy, "Smart contract enabled online examination system based in blockchain network," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2021, pp. 1–7.

[14] Y. Zhenming, Z. Liang, and Z. Guohua, "A novel web-based online examination system for computer science education," in *Proc. 33rd Annu. Frontiers Educ.*, vol. 3, Nov. 2003, pp. 7–10.

[15] P. H. B. Shinde, "Exam conduction and proctoring system using face detection," *Int. J. Sci. Res. Eng. Manag.*, vol. 6, no. 1, Jan. 2022, Art. no. 11444, doi: 10.55041/ijsrem11444.

[16] M. Z. Rashad, M. S. Kandil, A. E. Hassan, and M. A. Zaher, "An Arabic web-based exam management system," *Int. J. Elect. Comput. Sci.*, vol. 10, no. 1, pp. 1–7, 2010.

[17] T. M. Fagbola, A. A. Adigun, and A. O. Oke, "Computer-based test (CBT) system for university academic enterprise examination," *Int. J. Sci. Technol. Res.*, vol. 2, no. 8, pp. 1–7, 2013.

[18] J. Rooksby and K. Dimitrov, "Trustless education? A blockchain system for university grades1," *Ubiquity, J. Pervasive Media*, vol. 6, no. 1, pp. 83–88, Nov. 2019, doi: 10.1386/ubiq_00010_1.

[19] S. J. Pee, E. S. Kang, J. G. Song, and J. W. Jang, "Online test and management system using blockchain network," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 269–272, doi: 10.23919/ICACT.2019.8701891.

[20] X. Yang, S. Wang, F. Li, Y. Zhang, W. Yan, F. Gai, B. Yu, L. Feng, Q. Gao, and Y. Li, "Ubiquitous verification in centralized ledger database," in *Proc. IEEE 38th Int. Conf. Data Eng. (ICDE)*, Kuala Lumpur, Malaysia, May 2022, pp. 1808–1821, doi: 10.1109/ICDE53745.2022.00181.

MOHAMED ABDELSALAM received the master's degree in information technology from the Faculty of Computers and Information, Helwan University, Cairo, Egypt, in 2013, and the Ph.D. degree in information systems, in July 2018, with a focus on constructing virtual reality e-learning environment framework based on personalized learning. He is currently an Associate Professor with the Information Systems Department, Faculty of Commerce and Business Administration, Helwan University, Cairo. The master's degree project is on "A proposed framework for applying business intelligence to enhance ontology learning style." He has teaching experience of more than ten years in the areas of information systems. He has published several researches in various fields of information systems. His current research interests include data analytics, data mining, machine learning, e-learning solutions, data science, data warehousing, and blockchain.

MARWAN SHOKRY was born in Cairo, Egypt, in 1996. He received the bachelor's degree in commerce and business administration from the Business Information Systems Program, Faculty of Commerce and Business Administration, Helwan University, Cairo, in 2018. He is currently pursuing the master's degree in commerce and business administration witth Helwan University.

From 2018 to 2019, he was a Teaching Assistant with the Business Information Systems Program. He is a Full Stack Developer with the Software Department, Santeon Group Software Company. His current research interests include blockchain networks, cryptocurrency, university networks, and network security.

AMIRA M. IDREES is currently a Professor of information systems and data science with the Faculty of Computers and Information Technology, Future University in Egypt, Cairo, Egypt. She is also the Head of the Information Systems Department and the University Requirements Unit. She has been the Head of the Scientific Department and the Vice Dean of community services and environmental development with the Faculty of Computers and Information, Fayoum University. Her current research interests include knowledge discovery, text mining, opinion mining, cloud computing, e-learning, software engineering, data science, and data warehousing.