applied sciences

MDPI

Article

Blockchain-Based Quality Assurance System for Academic Programs

Mohammad Alkhatib *, Talal Albalawi and Fahman Saeed

Computer Science Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia; tsalbalawi@imamu.edu.sa (T.A.); faesaeed@imamu.edu.sa (F.S.)

* Correspondence: mhalkhatib@imamu.edu.sa

Abstract: Nowadays, technology is increasingly being adopted in different kinds of businesses to process, store, and share sensitive information in digital environments that include enormous numbers of users. However, this has also increased the likelihood of cyberattacks and misuse of information, potentially causing severe damage. One promising technology, which can provide the required security services with an improved level of efficiency, is blockchain. This research explores the use of Ethereum blockchain and smart contracts to create a secure and efficient quality assurance system (QAS) for academic programs. By utilizing blockchain and smart contracts, the proposed approach improves the integrity and reliability of sensitive information processed by the QAS, promotes transparency and governance, and reduces the time and effort required for quality operations. The current approach uses an additional access control layer to further enhance user privacy. Smart contracts automate various quality transactions and saves time and resources, and hence increases the efficiency of the QAS. The interplanetary file system (IPFS) is used to address the challenge of size limitations in blockchain. Additionally, this research investigates the use of various cryptographic schemes to provide robust security services at the application layer. The experimental results showed that the use of a hybrid cryptosystem relying on an Elliptic curve digital signature and AES encryption (AES_ECCDSA) outperforms other counterparts' cryptosystems using an RSA digital signature and AES encryption (AES_RSADSA) and Elliptic Curve Integrated Encryption Scheme (ECIES) in terms of speed. The performance results showed that AES_ECCDSA consumes 188 ms to perform the required cryptographic operations for a standard-quality document with a size of 8088 KB, compared to the 231 ms and 739 ms consumed by the AES_RSADSA and ECIES schemes, respectively. This study presents a prototype implementation of the blockchain-based QAS, which outlines the processing model and system requirements for key QAS processes. It has been found that the cost and time required for blockchain operations vary depending on the size of the input data—a larger data size requires more time and costs more to process. The results of the current study showed that the time delay for blockchain transactions ranges from 15 to 120 s, while the cost ranges from USD 50 to USD 400. This research provides evidence that blockchain and smart contract technologies have the potential to create a secure, efficient, and trustworthy QAS environment for academic programs.

Keywords: blockchain; smart contracts; privacy; security; integrity; trustworthiness; quality assurance

check for updates

Citation: Alkhatib, M.; Albalawi, T.; Saeed, F. Blockchain-Based Quality Assurance System for Academic Programs. *Appl. Sci.* **2024**, *14*, 4868. https://doi.org/10.3390/app14114868

Academic Editor: Gianluca Lax

Received: 28 April 2024
Revised: 29 May 2024
Accepted: 29 May 2024
Published: 4 June 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

A quality assurance system (QAS) is crucial in ensuring the effectiveness and reliability of academic programs in higher educational institutions (HEIs). The QAS provides systematic assessment and improvement of the various aspects of the educational environment, and thus, it is vital for monitoring and maintaining the overall quality of education in academic programs. The QAS involves various processes such as a rigorous assessment of the curriculum, students' performance, KPI analysis, and stakeholder surveys. The expected

outcomes of these processes are significant for decision-making and the development of improvement plans [1–3].

Ensuring the security of the sensitive information produced through the QAS is critical and has recently received increasing interest. Research studies have shown that cyberattacks and data breaches in HEI systems have been on the rise over the past decade [4].

Cybersecurity threats pose a significant risk to security and privacy in HEIs. Unauthorized manipulation of students' certificates, assessments, and learning materials, as well as the loss or unintended disclosure of sensitive personal data, are just a few examples of these threats. Additionally, plagiarism and copyright violations are also major issues faced by HEIs worldwide. In the digital world, threats to the QAS can arise due to both intentional and unintentional misuse of resources in addition to cyberattacks such as Distributed Denial-of-Service Attacks (DDoSs). DDoSs have become increasingly prevalent and can result in catastrophic consequences for the system resources. These attacks can compromise the confidentiality, integrity, and availability of the system, thus posing a significant threat to its overall security and stability [5–8].

Therefore, finding an efficient and secure way to store, share, and process the sensitive quality files produced by the QAS is highly needed. To counter related threats and cyberattacks, the current research attempts to establish a reliable and trustworthy environment that enables the safe exchange and cooperative development of quality files while preserving privacy and security. Past research studies have emphasized the importance of developing such environments and finding practical solutions to improve the efficiency of QASs [9–11].

The current research investigates the adaptation of the distributed ledger technology, known as blockchain, to develop a secure and efficient QAS. Blockchain is one of the cutting-edge technologies that can enhance the security and governance of a QAS via its powerful security features. It can provide transparency, traceability, immutability, and secure sharing and hence contribute to establishing trustworthiness and a reliable environment for quality operations [12–14].

Many research studies have explored the advantages of using blockchain to offer security services for several processes performed by HESs. Blockchain, along with related technologies such as smart contracts, has been implemented to create a secure system that ensures the integrity and availability of students' certificates. Furthermore, blockchain has been used to improve users' privacy within HESs. Additionally, previous research studies utilized the traceability features of blockchain to enable the effective tracking and verification of sensitive information related to learning records, student scores, and work experience. Moreover, one of the key benefits of blockchain in HESs is its ability to enhance the governance and management of various processes [15–19].

Despite the potential advantages that blockchain and smart contracts offer in terms of enhancing security and governance, their potential to support a QAS in academic programs has not been fully explored. This research aims to address this gap by proposing a blockchain-based QAS for academic programs that can effectively control and manage quality operations, while also creating a transparent and trustworthy environment for processing quality-related data and transactions. The proposed approach represents the first attempt to develop a blockchain-based system to secure and manage quality assurance processes. Moreover, this research investigates three well-known cryptographic schemes, which are the RSA digital signature algorithm (DSA) with AES encryption, the Elliptic Curve DSA with AES encryption, and the Elliptic Curve Integrated Encryption Scheme (ECIES), to provide additional security services at the application layer. The cryptographic schemes are implemented and compared in terms of time consumption to find the best one to be integrated into the QAS.

The current research employs the interplanetary file system (IPFS) to address the storage space limitations of blockchain. The IPFS is a distributed file sharing and storage protocol that aims to provide safe and faster storage environments on the web. The IPFS uses cryptographic hash functions to produce a unique hash code for each file and its related blocks. The content-based hash can be used to search for files that might be distributed

on several nodes in the network. In comparison with the traditional distributed storage techniques that require storing multiple copies of the same file on different servers in the network, IPFS can significantly reduce the redundancy of data stored across the network. This represents a considerable saving in resources. Furthermore, the IPFS can enhance the performance of data retrieval, because it uses a distributed hash table (DHT) to locate the nearest copy of the file so that it can be efficiently retrieved. Also, the IPFS can avoid the risk of a single point of failure and hence preserve the availability of data [20]. Additionally, by integrating the IPFS with a blockchain, such as Ethereum, the scalability issues of blockchain can be alleviated, since only essential transaction metadata are stored on the blockchain, while large files are stored off-chain. The use of the IPFS can save blockchain space and enhance the overall network performance [21].

The following sections present relevant research works, the proposed model, experimental results and discussions, and finally, the conclusion and future research directions.

2. Related Work

Quality assurance in HEIs refers to the practices that aim to meet academic standards, achieve learning outcomes, and improve the overall quality of academic programs [3]. An effective QAS plays a vital role in enhancing the quality of teaching and learning, and hence, it improves the knowledge and skills earned by the programs' graduates. In today's knowledge-based economy, advanced human capital is very important for economic development and essential for a nation's competitive advantage [22]. HEIs and standardization organizations are committed to ensuring the quality of education and academic accreditation. To achieve this, they have developed specific quality standards, criteria, and practices [23,24].

QASs in HEIs strive to meet established standards and criteria in all aspects of the academic environment. This includes teaching, learning, assessment, decision-making, and improvement planning processes. As a result, QASs produce and process sensitive information. Effective communication among stakeholders that takes security and privacy issues in QASs into consideration is necessary [9].

In the last few decades, educational institutions have faced various information security risks. It was found that there is a significant increase in risks to scientific integrity, including unethical activities such as faking peer review processes, plagiarism, fabrication and falsification of research materials, and other forms of misconduct. Research results found that the estimated cost for handling such misconduct cases is around USD 110 million annually. In addition, these unethical activities and misconduct have a severe impact on the educational and research environment. Therefore, it is essential to implement effective solutions to preserve integrity and create a secure and trustworthy educational and research environment [6].

A recent study has shown that maintaining privacy is crucial in the fields of education and research [7]. The study presented a system that enables real-time data analysis while safeguarding user privacy. The proposed system ensures the anonymity of the extracted data from the learning management system (LMS), preventing personal information from being exposed during data analysis. However, the system does not address other significant concerns such as the integrity, accountability, transparency, and trustworthiness of educational and research materials. Additionally, it does not provide a means of tracking learning and research resources and quality reports.

In a research paper [23], the idea of an interactive online repository for learning resources was put forward. This repository would allow teaching staff to work together on creating educational materials. While the paper addressed collaboration and sharing of resources, it did not touch on the crucial need for security measures to protect these assets. Along with a secure environment for these materials, the authors emphasized other key pillars of a quality educational system, such as transparency, integrity, validity, and fairness in assessing students [8].

During their discussions, researchers identified key factors that are crucial to the success of international university cooperation. They determined that effective collaboration between universities and other stakeholders is essential for creating a high-quality education and research environment [10]. As a result, it has become increasingly important to establish a secure and practical platform that facilitates the sharing and development of educational materials and scientific research to promote continuous improvement within higher education systems.

In [11], the researchers developed a trusted and transparent ecosystem for sharing personal data called "myneData". The proposed ecosystem aims to address some challenges related to legal obligations and technological limits. Another study aimed at developing an effective and secure environment for sharing sensitive information in HEIs was presented in [24]. The researchers introduced a model that enables secure and distributed configuration, authorization, and management in the cloud-based Internet of Things.

Numerous studies have explored the potential of cutting-edge technologies like blockchain and smart contracts to create a secure and efficient framework for sharing sensitive information, promoting collaborative development, and streamlining key processes in higher education institutions (HEIs). For example, one recent study [19] leveraged the dependable distributed ledger and promising smart contract technology to establish a trustworthy distributed platform for issuing academic certificates and transcripts. In a separate investigation, researchers developed a blockchain-based system that verified the authenticity and integrity of students' transcripts for hiring organizations, using the immutable nature of blockchain to ensure the accuracy of students' records [25].

In [26], a group of researchers implemented blockchain technology to create a learning log platform and streamline the transfer of academic records between higher education institutions (HEIs). By utilizing blockchain, HEIs were able to securely and efficiently exchange student grades and academic records, particularly for universities with student mobility programs. Another studies [27,28] developed a trusted framework using blockchain technology to verify students' achievements and connect them with potential employers. This enabled employers to easily identify qualified candidates for employment.

Studies have revealed that the implementation of smart contracts utilizing blockchain technology has the potential to establish a secure and streamlined electronic platform for higher education institutions (HEIs) [29]. This platform automates the assessment and issuance of credentials, while providing a transparent and reliable environment to store sensitive data produced by higher education systems (HESs). Additionally, ref. [7] proposed a secure blockchain-based system design that enables collaboration among stakeholders in HEIs to improve educational materials, such as course slides and tutorials. Another research endeavor explored the anonymity feature of blockchain, which can enhance the privacy of users in HEIs [30]. It was observed that utilizing blockchain technology can provide users with greater control over their personal information and limit the exposure of identifiable information.

Blockchain is adopted by various modern systems to improve security and efficiency. The researchers in [31] investigated the use of blockchain and smart contracts to improve an airport security system. The research findings showed that adopting smart contracts can reduce the complexity and enhance the efficiency of airport security processes. Another study in [32] adopted blockchain and the IoT for an efficient system for decentralized and secure data recording. The proposed blockchain-based system maintains users' privacy and reduces operational costs.

Blockchain technology provides robust services such as data security, transparency, and decentralization. Since the introduction of Bitcoin in 2008 [33], blockchain technology has evolved significantly, leading to the development of various types of technologies that are tailored to different uses and requirements. In general, blockchains can be categorized into three types: public, private, and consortium (or federated) blockchains. Each type of blockchain offers distinct advantages but has its own limitations.

Public blockchains are open, decentralized networks, where anyone can participate and validate transactions. Compared with other blockchain types, public blockchains are characterized by transparency and security features. Private blockchains, on the other hand, are restricted networks, where access is limited to a specific group of participants. This sacrifices the level of decentralization and transparency, which can lead to concerns about trust and security. Consortium blockchains blend elements of both public and private blockchains by allowing a predefined group of participants to govern the network. Although consortium blockchain has a higher level of trust and security in comparison with private blockchains, it still inherits some disadvantages of the decentralized approaches. For example, consortium blockchains have limited decentralization levels, which hinders them from providing fully trustworthy and decentralized environments. Additionally, the complex governance structures in consortium blockchains can lead to significant obstacles to decision-making and increase the time consumed by blockchain transactions [34–36].

The current study adopts Ethereum, one of the most widely used public blockchains. This enables the utilization of transparency, decentralization, and security features, which are essential requirements for QASs. Additionally, Ethereum supports smart contracts, which enables the automation of transactions, the efficient management of operations, and the development of decentralized applications (dApps). The current approach suggests adding a layer of authentication, supported by cryptographic algorithms, to the proposed blockchain-based QAS to improve privacy and security services.

Furthermore, previous research has not fully explored the potential of utilizing blockchain and smart contracts to enhance the security and governance in quality assurance processes. In this study, we leverage blockchain technology to create a dependable and secure platform for sharing, collaborating, and validating sensitive quality information and reports. Our aim is to establish a trustworthy environment that prioritizes transparency and accountability.

In the next section, the proposed blockchain-based model for securing and managing QAPs and related information in HEIs is presented.

3. The Proposed Blockchain-Based QAS

The proposed blockchain-based system aims to utilize the security features of blockchain technology to offer a secure ecosystem for sharing and verifying quality information and reports.

This section introduces the blueprint and simple prototype implementation of the proposed blockchain-based ecosystem for QAPs. It represents a proof of concept and shows the initial framework and principles that will guide the development of the ecosystem. The aim is to create an efficient and secure system that can support various quality assurance activities using blockchain and smart contract technologies.

3.1. High-Level Description

Figure 1 provides a comprehensive overview of the proposed QAS, which utilizes blockchain technology to ensure transparency, integrity, and secure information sharing among various parties. The QAP entails specific roles and responsibilities for quality members, accreditation authorities, independent reviewers, deanship of quality, instructors, course coordinators, advisory committees, and other departmental and college members. The adaptation of blockchain technology offers the necessary security measures to guarantee the success of the QAP.

The proposed solution offers clients a user-friendly web application that enables them to seamlessly engage with the blockchain technology and carry out various quality assurance tasks with the utmost security and transparency. The web application implements stringent authentication and authorization protocols for users, which function as a robust access control layer, ensuring that users are granted appropriate permissions according to their designated role and can only perform relevant actions.

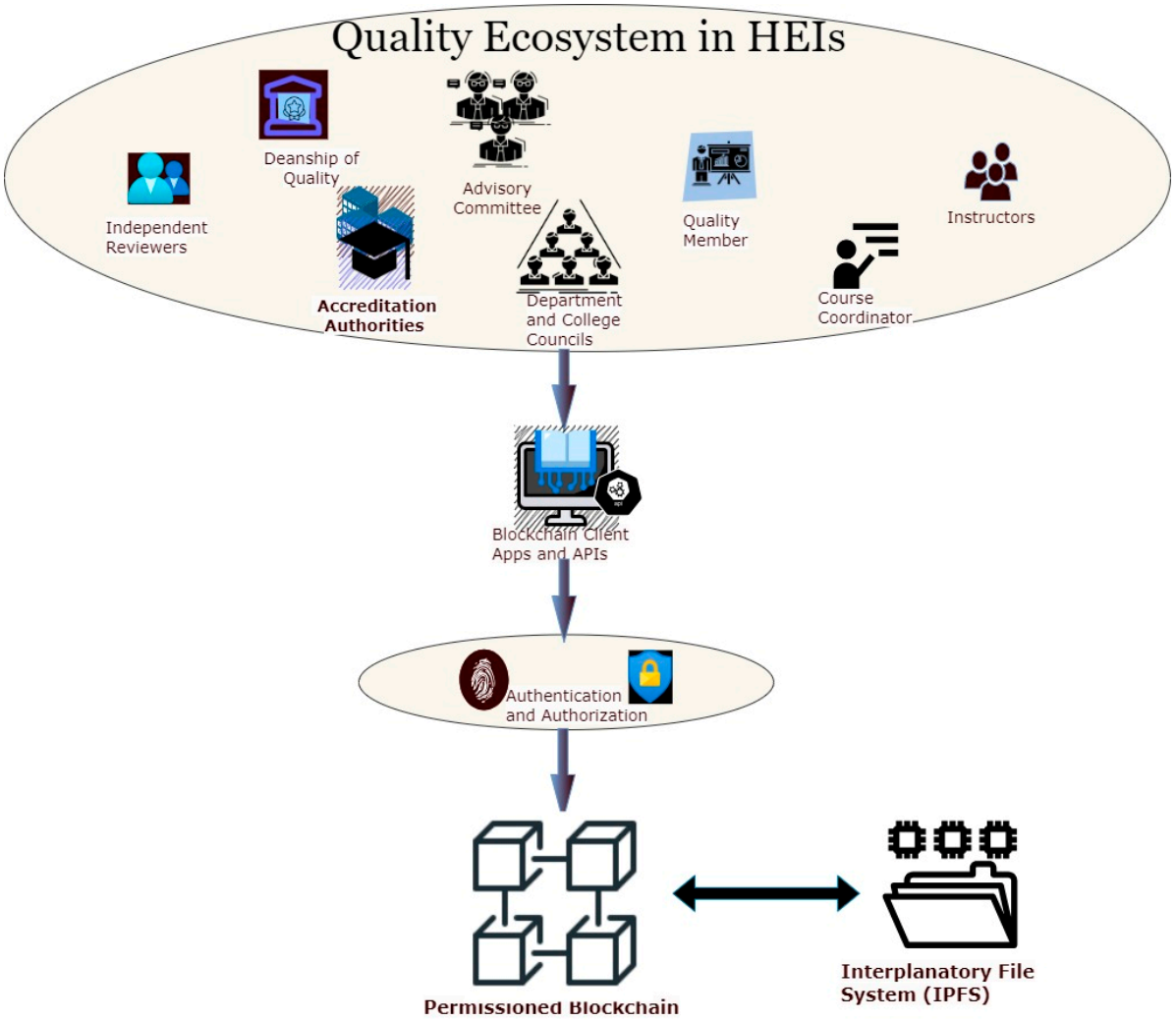


Figure 1. High-level description of proposed blockchain-based quality assurance ecosystem.

The interface of the web application enables users within the quality assurance ecosystem to engage with the blockchain via an application programming interface (API). Users can undertake various tasks, including storing, sharing, and verifying quality reports, while benefiting from the security features provided by blockchain technology. The proposed ecosystem utilizes a permissioned blockchain to meet the security requirements of the QAS, thereby limiting certain actions to privileged users within the blockchain-based quality ecosystem.

It can be noticed from Figure 1 that the distributed storage technique known as the interplanetary file system (IPFS) is used to solve storage limitations in the blockchain technology. Through using the IPFS, actual data and reports can be stored in the file system, where the hash code of the file is stored on the blockchain. This can offer more space to store quality data, which cannot be provided by the blockchain, and improve the performance of blockchain operations.

3.2. Organizational Structure of Quality Assurance Ecosystem

This section aims to provide a comprehensive understanding of the proposed quality assurance ecosystem based on blockchain technology. Figure 2 illustrates the organizational structure that defines the roles and responsibilities of users in the ecosystem.

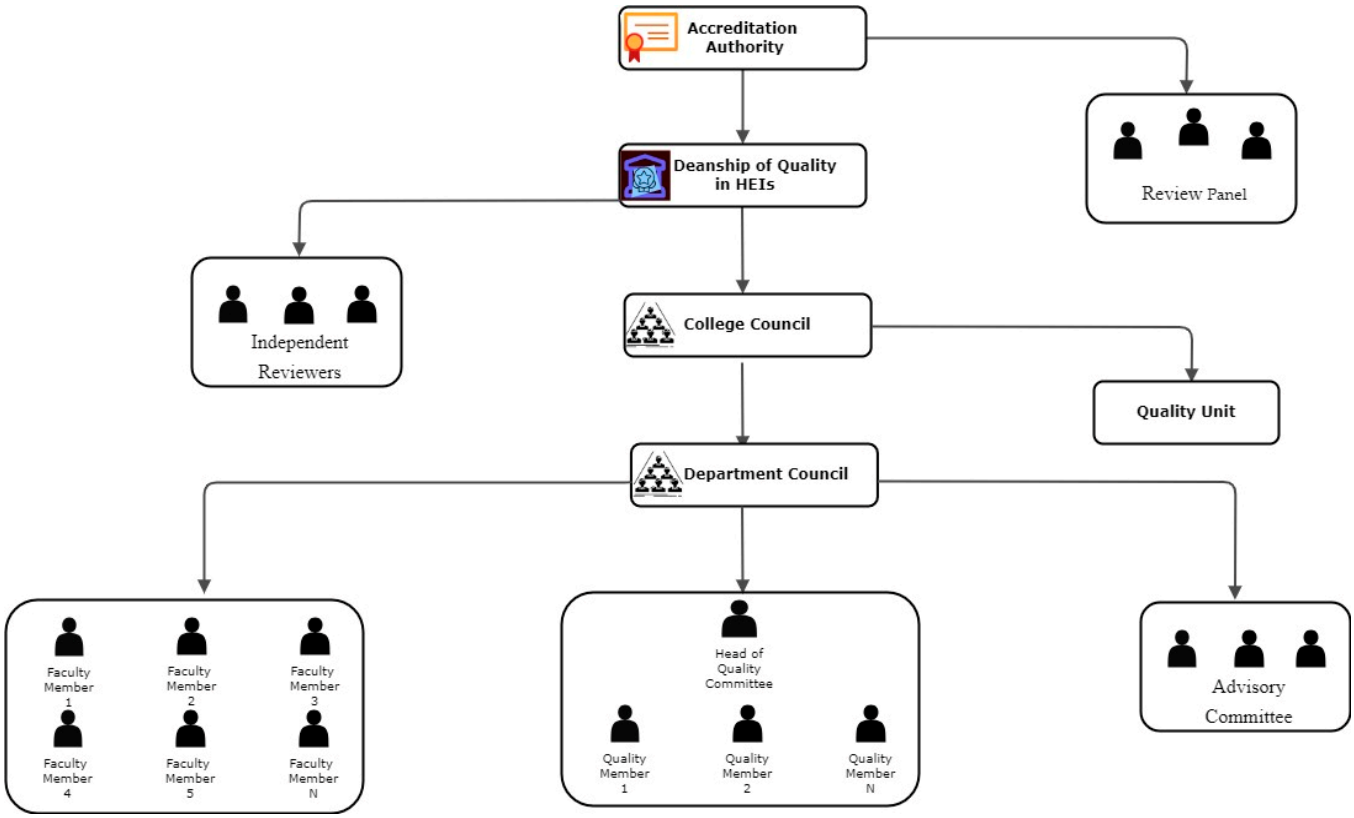


Figure 2. Organizational structure of quality assurance ecosystem.

The accreditation authority is at the top level of the hierarchy and has the highest level of authority. Authorized members of a specific accreditation authority can access quality reports from all academic institutions and programs that are accredited by the authority or seeking its accreditation. Additionally, the accreditation authority can access evaluation reports submitted by its review panel. One critical responsibility of the accreditation authority is to register the official email addresses of all users in the review panels and HEIs (higher education institutions), represented by the deanship of quality that belongs to them. The developers of the blockchain-based ecosystem must register official email addresses for well-known accreditation authorities worldwide. In the future, a new accreditation authority can be registered and approved by an existing authority.

The next level in the organizational structure's hierarchy is the deanship of quality in HEIs. The quality deanship in a particular university can access and approve all quality reports submitted by colleges within the university and the independent reviewers assigned by the deanship of quality. Authorized users' email addresses should be registered in the blockchain-based ecosystem by the deanship of quality in each university.

The college council is the next level in the hierarchy. Similar to the previous levels, the college council can access and approve quality reports submitted by college members and is responsible for registering email addresses for all department councils and college quality unit users.

At the bottom of the hierarchy is the department council, which can access and approve reports submitted by all quality committee members, faculty, and advisory committees within the department. The department council is responsible for registering email addresses for the department's users.

It is evident from the organizational structure of the proposed ecosystem that there are several cascading levels of authorities, and each level can observe and register users in the next level of the organizational structure.

Table 1 outlines the roles and permissions for different users within the ecosystem based on blockchain technology. Instructors are authorized to create, edit, view, approve,

and comment on their course reports. However, other parties within the ecosystem can only view, comment on, or approve the reports submitted by instructors.

Table 1. Roles and permissions in the proposed blockchain-based ecosystem.

Roles Permissions	Faculty Member (Instructor)	Quality Committee Member	Department Council Member	College Council Member	Accreditation Authority Member	Deanship of Quality Member	Reviewer (Evaluator)	Advisory Committee Member
Permissions related to course reports								
Create course report	√							
View course report	√	√	√	√	√	√	√	√
Edit course report	√							
Comment on course report	√	√	√	√	√	√	√	√
Approve course report	√	√	√	√				
Permissions related to quality reports (APRs, LO assessments, KPI analysis, etc.)								
Create quality reports		√						
View quality reports	√	√	√	√	√	√	√	√
Edit quality reports		√	√	√				
Comment on quality reports		√	√	√	√	√	√	√
Approve quality reports		√	√	√		√		
Permissions related to user management								
Register users			√	√	√	√		
Cancel user registrations			√	√	√	√		

In the case of quality reports, such as APRs, survey reports, learning outcome assessment (LO) reports, KPI analyses, and others, quality committee members within the department have the right to create, edit, view, approve, and comment on them. Other parties in the ecosystem can also view, comment on, or approve the reports, but they cannot create them, as it is the responsibility of the quality committee members in the department. Faculty members can only view the quality reports that have been approved by the department council.

Regarding user management permissions, department and college councils, deanships of quality representatives, and accreditation authorities are authorized to register and cancel user registrations.

3.3. The Blockchain-Based Model for QAPs

In this section, we will discuss a proposed model for quality assurance processes (QAPs) that utilize blockchain and smart contract technologies. The model explains how these technologies can be used to perform different QAPs. Figure 3 presents the proposed model.

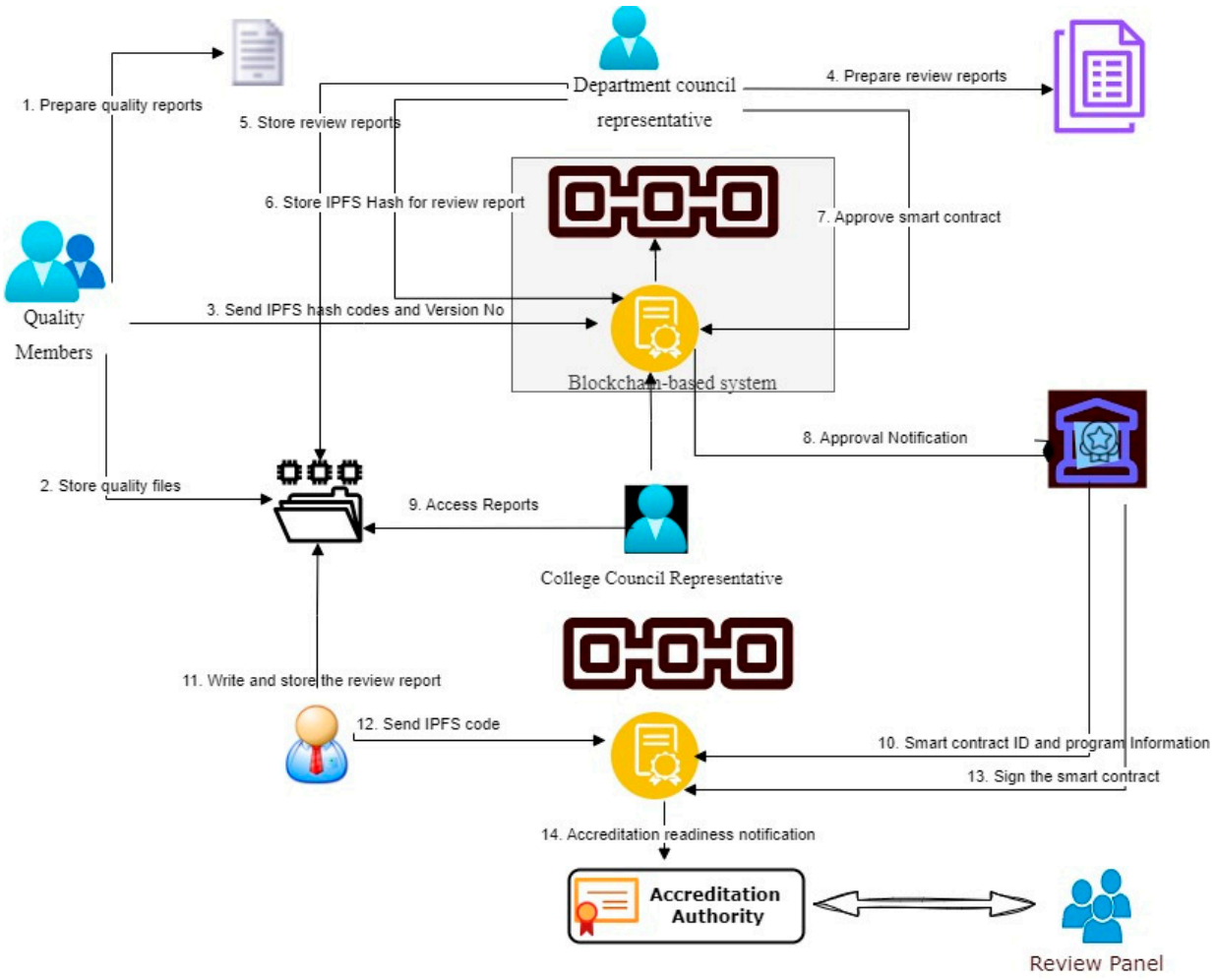


Figure 3. Proposed model for blockchain-based quality assurance ecosystem.

During the first stage, quality committee members and instructors prepare quality and course reports. The quality reports are stored offline using IPFS technology, while the hash code and version number are input to the smart contract. Representatives of the department council prepare review reports and comments on the quality files prepared by quality members. Like quality reports, review reports will also be stored offline in the IPFS, and hash codes will be input into the smart contract, which will be signed by the departmental and college council representatives. Once approved, all quality files' transaction and hash codes are stored in the blockchain to ensure the integrity and availability of sensitive quality reports.

College council members can access reports submitted by academic departments, while the deanship of quality can access reports prepared by all colleges within the university. After signing the smart contract, the deanship of quality will receive a notification. The ID of the smart contract signed by the college and the program information are input to another smart contract at the university level.

An independent reviewer will write review reports that are stored in the IPFS, while the hash codes are input to the smart contract, which will be signed by the higher education institution (HEI), represented by the deanship of quality. Once the HEI signs the smart contract, it is equivalent to the official approval of quality documents. As a result, the accreditation readiness notification is sent to the accreditation authority and panel review.

The proposed system presented in Figure 3 leverages blockchain and smart contract technologies to offer distinct advantages over traditional QASs. In the proposed blockchain-based system, every transaction and update to quality documents is authenticated and

recorded on an immutable ledger, ensuring transparency and traceability. Furthermore, the use of smart contracts enables the automation of QAS processes and enforces compliance with predefined policies. It is worth mentioning that the use of blockchain makes it virtually impossible to tamper with quality records, because any attempt to alter quality records would require consensus of all parties across the network. This significantly reduces the risk of human error and fraud and preserves the integrity of sensitive quality data. In contrast, traditional QASs are more centralized and vulnerable to various attacks, such as unauthorized access, a single point of failure, and data manipulation and misuse. These QASs typically rely on conventional databases that can be altered by users with sufficient access privileges, creating potential security issues. Additionally, traditional QASs require intensive human intervention and often lack the automated enforcement mechanisms provided by smart contracts. For example, these systems require some officials to conduct manual checks and updates to ensure compliance with quality standards. This can lead to inefficiencies and increased administrative overhead.

In summary, the current blockchain-based QAS provides improved levels of security, transparency, and automation compared to traditional quality systems, which suffer from serious security and efficiency issues.

The next section presents the process model for user enrolment in the proposed QAS and related user enrolment and registration operations.

3.4. The Process Model for User Enrolment

This section outlines the process model for user login in the proposed blockchain-based quality assurance ecosystem. Figure 4 presents the main processes and actions taken during user enrolment or login. This process model applies to all users who seek enrolment in the platform.

To start, the user needs to access the web application. If the user already has an account, they can log in using their credentials, which include their public wallet address, email address, and password. Once authenticated, the user can log in to the system and perform quality assurance activities based on their role and permissions, as presented in Table 1.

However, if the user does not have an account, he needs to sign up and create one, along with a blockchain wallet. The user must have an email address registered in the system by a higher level of authority to do so. If the user is not registered, the blockchain wallet creation process will not proceed.

Assuming that the user has a valid email address, a verification request will be sent to that email address. Once the user is verified, he can proceed to create a blockchain wallet. Otherwise, his request will be declined. The public key represents the user's address in the blockchain ecosystem and ensures privacy, since their actual identity will be hidden from other users, except from the higher level of authority, according to the organizational structure of the quality assurance ecosystem. It is essential to keep the private key of the user's wallet secret.

Then, the user should fill in the registration form, including his public key and email address. A copy of the user's information is sent to the higher level of authority to keep a record of authenticated users containing their email and wallet addresses. Eventually, the user can proceed to log in using his credentials.

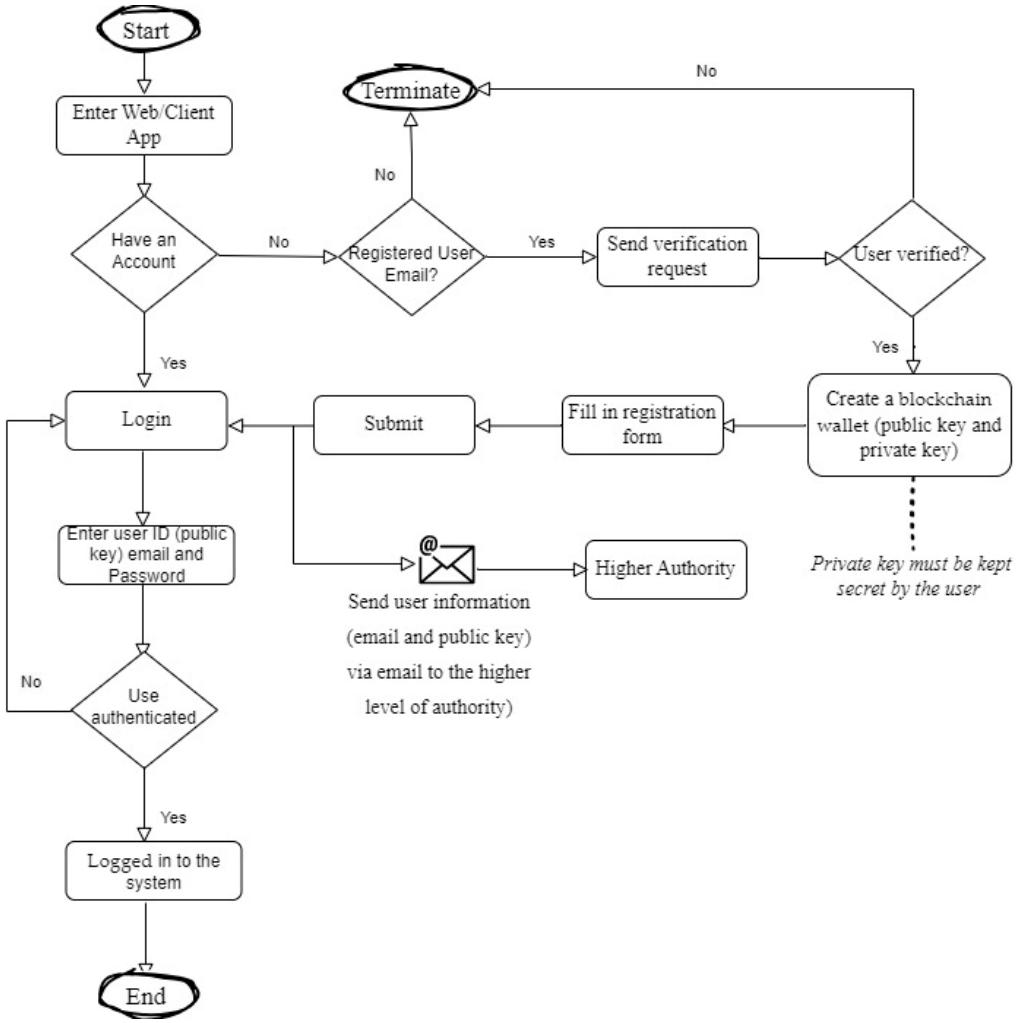


Figure 4. The process model for user logins in the blockchain-based platform.

3.5. System Requirements for Internal QAPs

This section presents the steps and requirements for conducting internal QAPs within HEIs. The process involves creating, reviewing, storing, and approving quality documents. To facilitate the approval process, smart contract technology is utilized, and an IPFS is used to store quality files and address the size limits of the blockchain.

Figure 5 depicts the sequence diagram for internal processes conducted by various entities involved in the QAS. The diagram also highlights essential system components such as smart contracts and the IPFS.

Quality members can create quality reports and store them in the IPFS. The reports' hash codes and version numbers are then input into the smart contract. Department council representatives can retrieve quality reports and request revisions. The review forms and modified quality reports are stored using the IPFS, and the hash code is input to the smart contract.

Representatives from college and department councils use their private keys to sign the contract. By signing the smart contract, the quality reports are officially approved. Once the contract is executed, an automatic notification and the necessary data to access the quality reports are sent to the deanship of quality in the university.

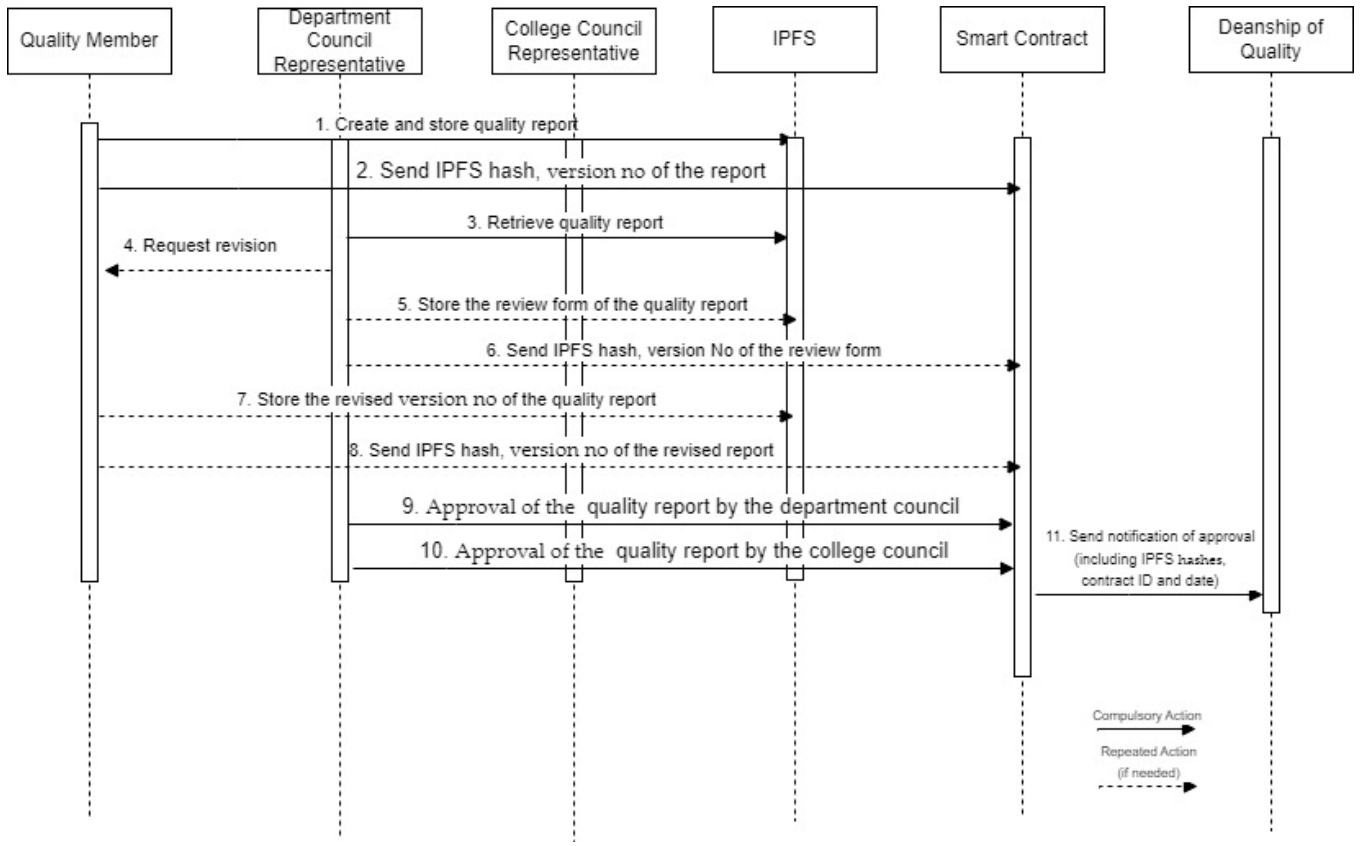


Figure 5. The sequence diagram for internal QAPs.

The next section outlines the system requirements for academic program accreditation processes.

3.6. System Requirements for Accreditation Processes

The process of accrediting a program is a crucial part of the quality assurance system (QAS). This section outlines the requirements for a blockchain-based system for program accreditation. Figure 6 depicts the sequence diagram for the processes and actions that are carried out by the entities involved in the accreditation process.

The system uses IPFS technology to store quality files and smart contracts to perform transactions. The accreditation process involves program and quality deans from a particular HEI, the accreditation authority, and independent reviewers. All parties interact with each other during the program accreditation process.

The first step involves the program representatives creating and storing accreditation requirements and reports using the IPFS. The hash code and program information are then input into the smart contract. In the next stage, the quality deanship requests an independent review. The review request form includes the smart contract ID and the hash code of the program files that are stored using the IPFS. The reviewer can access the program quality reports by searching using the hash code. The reviewer then creates and stores the review report, with the hash code and version number being input into the smart contract.

Once the review report is complete, the quality deanship representative approves the accreditation request and signs the smart contract. Once the smart contract is signed, the formal request for accreditation, along with related quality reports, is automatically sent to the accreditation authority. All transactions and quality reports are registered on the blockchain to ensure protection from manipulation or falsification. The blockchain also enables easy tracing of all transactions and quality documents.

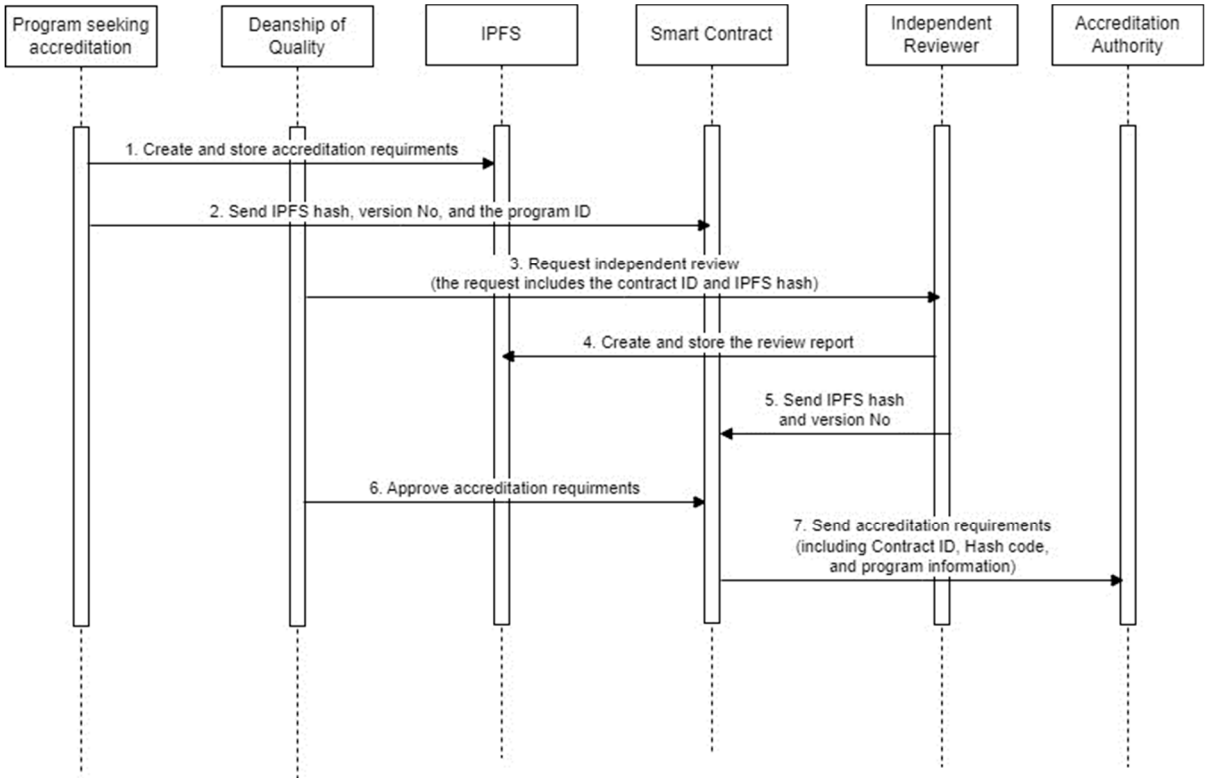


Figure 6. The sequence diagram for the program accreditation process.

Using blockchain technology ensures the confidentiality of users involved in the accreditation processes. For instance, the personal information of independent reviewers is not exposed to program or college representatives because they will be using the blockchain platform through their wallet addresses or public keys.

After presenting a basic prototype implementation, the following section discusses the security features and efficiency improvements that can be achieved by the proposed blockchain-based platform for QAPs.

3.7. Implementation Environment

3.7.1. Ethereum Blockchain and Smart Contracts

The proposed blockchain-based QAS uses the well-known Ethereum blockchain and smart contract technologies. The blockchain is public, so it can provide more security and transparency levels. Moreover, there is an additional authentication and access control layer imposed by the web system to control users and make sure that only authorized users can perform transactions in the QAS, and each user can have permissions as per his role, as specified in Table 1.

The Solidity programming language was used for implementing the smart contracts on the Ethereum Virtual Machine (EVM), while the Truffle development framework was used to facilitate the smart contract development and testing. The Metamask was used to allow users to access their Ethereum wallet and perform transactions through the QAS. To test the system, the known Rinkeby test network was utilized to avoid incurring actual Gas costs. To evaluate the blockchain-based QAS performance, the current study used the average block confirmation time, while the cost was estimated using the Gas fees offered to miners, as described in the next section.

The following code was used to develop the smart contract for signing quality reports. As previously mentioned, signing the smart contract represents official approval of the quality reports by the signer, and thus a notification, including the hash code of the report, the version number, and the owner's information and his signature, is sent to other concerned parties in the QAP to take necessary actions. The smart contract has three inputs:

the hash code of the quality report, the version number of the document, and the wallet address of the signer. Once the contract is signed, the function that sends the notification is called immediately. The source code file for developing the smart contract can be accessed through [37].

3.7.2. Methods to Evaluate the Performance and Resource Consumption Features of the Proposed Blockchain-Based QAS

In order to evaluate the features of the proposed blockchain-based QAS, this study utilizes performance and resource consumption metrics. Performance is assessed by calculating the time delay for blockchain transactions, typically represented by the average block time. In Ethereum blockchain, the block time refers to the duration that it usually takes for miners to solve the cryptographic puzzle required to add a new block to the blockchain. In simpler terms, it is the time taken to confirm a particular blockchain transaction. The block time is a crucial factor that affects the transaction speed and, consequently, overall performance. On the other hand, the resource consumption is estimated by evaluating the Gas fees and cost for Ethereum blockchain transactions. The Gas is a measurement unit that estimates the amount of computational effort required to execute smart contracts and blockchain operations. The Gas fees are offered for miners as an incentive to process blockchain transactions. The fee is calculated via multiplying the Gas price by the Gas limit, which is the total amount of Gas that the user is willing to spend on the blockchain transaction [38].

3.7.3. Implementing Cryptographic Algorithms for Enhanced Security in QMS

The current research investigated the use of various cryptographic algorithms to provide confidentiality, integrity, and non-repudiation services at the application layer. This aims to make all users confident that sensitive quality information is confidential and not manipulated by unauthorized parties. Moreover, the provided security services, in particular digital signatures, aim to ensure that the user who created and signed the quality report cannot deny his responsibility about that report.

To provide confidentiality, quality reports are encrypted using AES before sending them to other parties or storing them on any storage areas of cloud service providers. On the other hand, integrity and non-repudiation services were provided through digital signatures. The current research applied two popular digital signature algorithms (DSAs), which are the Elliptic curve cryptography DSA (ECCDSA) and RSA DSA. It has been found that the ECCDSA takes less time to generate the signature and hence achieves better performance. The rationale behind the enhanced performance level for the ECCDSA is that it can provide the desired security level while using much smaller key sizes compared to other public key cryptosystems. This means that the ECCDSA needs to perform less computations and hence consumes less time. The used encryption scheme is depicted in Figure 7.

As can be noticed from Figure 7, the implemented encryption scheme utilizes the ECCDSA to digitally sign the sensitive quality files. The use of digital signatures aims to ensure the integrity of such sensitive files and prevent source repudiation behaviors. This research study implemented both the RSADSA and ECCDSA. The later scheme was adopted because it has less computational complexity and takes less time. The code used to implement the ECCDSA to sign and encrypt quality files can be accessed through [37].

The following section briefly describes the GUIs of the proposed QAS.

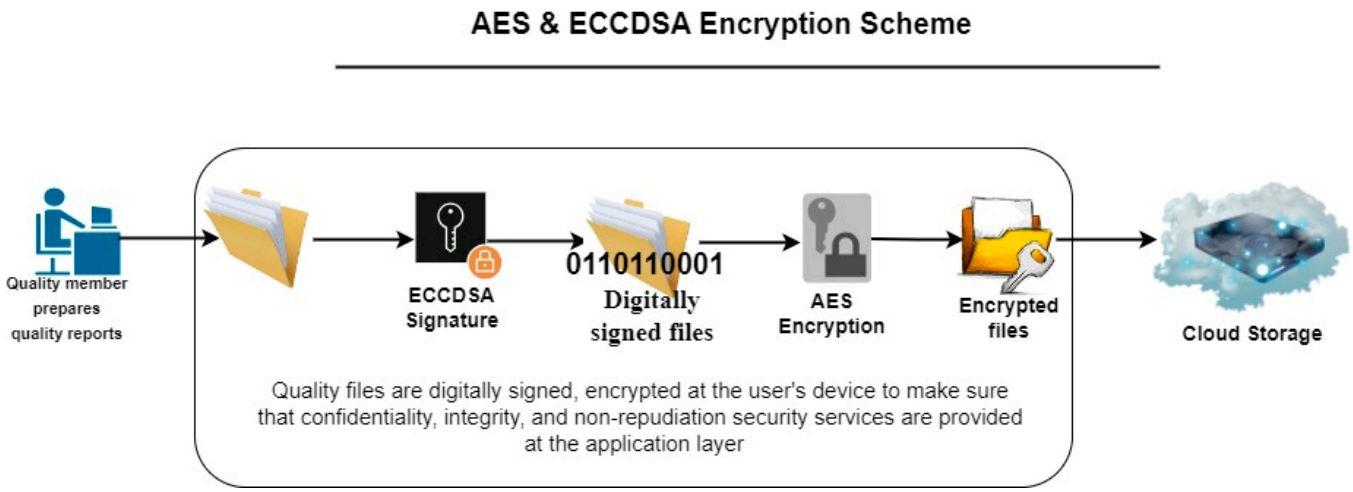


Figure 7. Adopted encryption and digital signature scheme.

3.7.4. Developing the GUIs of the Proposed QAS

We used javascripts and HTML to develop the web application interface. For the integrated development environment (IDE), a visual studio was used to write the HTML and Javascript codes.

Figure 8 shows the login interface for the proposed blockchain-based QAS. The user needs to login using his wallet ID, email address, and password, as previously discussed in the process model presented in Figure 8.

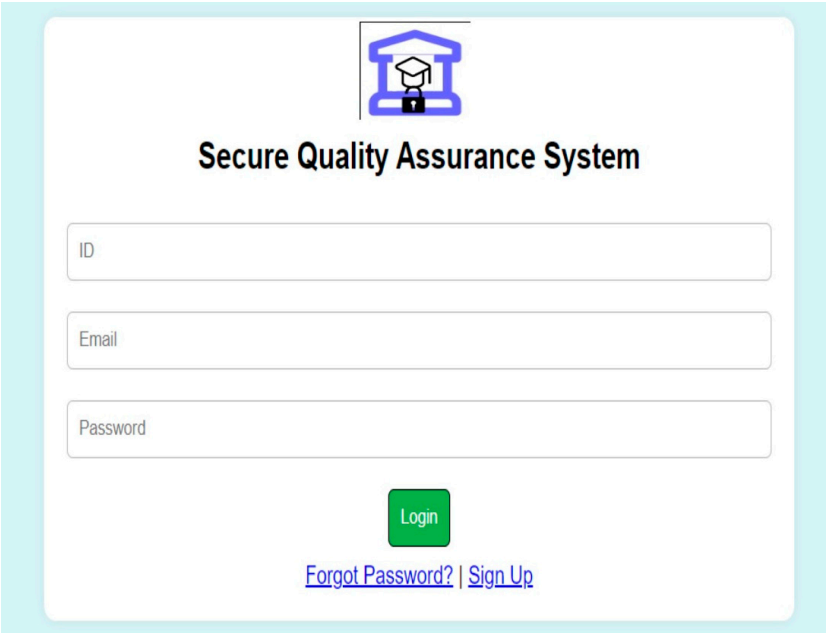


Figure 8. Login interface for the QAS.

The following section introduces the experimental results and analysis in terms of the performance and cost of the blockchain transactions and cryptographic operations, along with elaborations of the main research findings.

4. Experimental Results and Discussion

This section introduces the experimental results for the proposed blockchain-based QAS and cryptographic schemes. The results mainly show the time delay and cost of

the blockchain transactions and the time requirements for the different cryptographic operations required to provide security services for quality files.

4.1. Time Delay and Cost of Blockchain Transactions

This section presents the results in terms of the estimated Gas fees and costs of Ethereum transactions. Additionally, the estimated time delay for block confirmation is calculated. We assume that the input size of the transaction data ranges from 200 bytes to 1600 bytes. Equations (1) and (2) are used to calculate the cost and time delay, respectively. The results are presented in Table 2.

$$\text{Estimated cost (USD)} = ((\text{Gas Unit} \times \text{ETH})/100) \times \text{EX} \quad (1)$$

where ETH is the Ethereum Gas price and is generally denoted in Gwei, and EX is the real-time exchange rate for ETH to USD.

$$\text{Estimated Time delay (in seconds)} = \text{No. Blocks} \times \text{BlockTime} \quad (2)$$

We assumed that the average block time is 15 s.

Table 2. Time consumption results for the cryptographic operations with blockchain transactions.

Data Size (Kilobytes)	Time Consumption of Cryptographic Schemes with Blockchain		
	AES_ECCDSA	AES_RSADSA	ECIES
400 KB	30.036	30.42	30.150
800 KB	60.107	60.124	60.282
1200 KB	90.188	90.231	90.739

Figure 9 presents a comparison between the time delay (secs) and cost (USD) for blockchain transactions on quality files of different sizes. By observing the experimental results, it can be noticed that there is a direct relationship between the costs and time delays for blockchain transactions. Moreover, both the time delay and cost values increase as the file size increases. Consequently, the incorporation of IPFS technology to downsize the data that are kept in the blockchain becomes crucial in reducing the time delay, saving transactions costs, and boosting the overall performance of blockchain transactions.

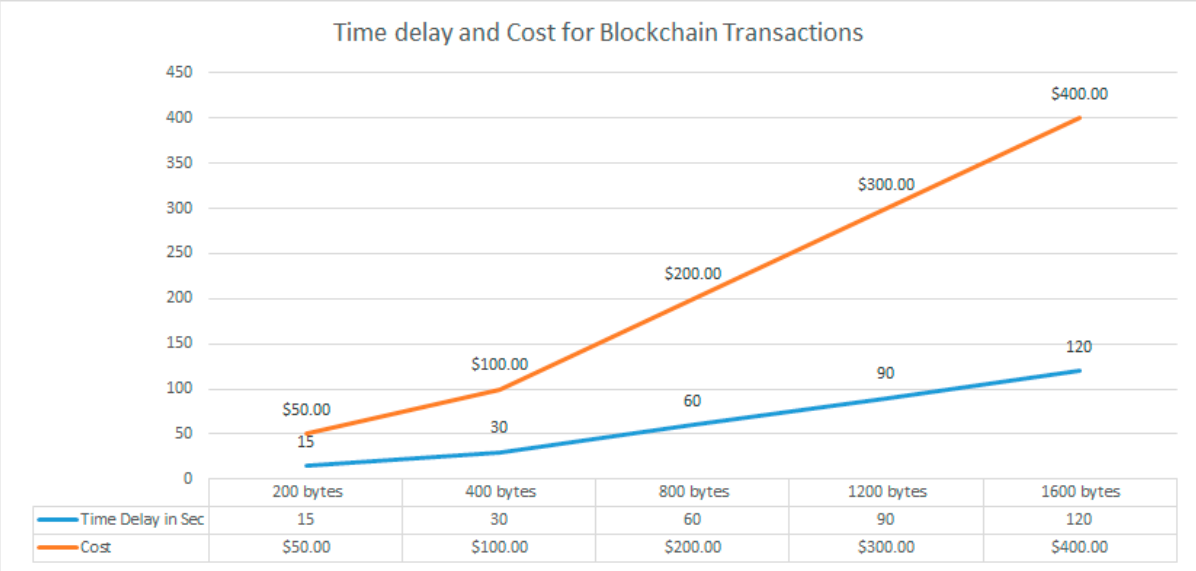


Figure 9. Time delay and cost of blockchain transactions on quality files of different key sizes.

The next section presents a deep analysis of the time consumption results and comparisons between the three cryptographic schemes. This aims to highlight the scheme that achieves the best performance level.

4.2. Time Consumption of Cryptographic Operations

The experiments conducted in this research implemented three cryptographic schemes. This aims to provide the required security services to protect sensitive quality information produced by the QAS. In particular, the experiments implemented the ECCDSA and RSADSA to provide digital signatures. After the quality files were digitally signed, they were encrypted using the AES algorithm to preserve the confidentiality of the content. Additionally, the current study investigated the implementation of the ECIES scheme to provide both authentication and confidentiality. Table 3 presents the time consumption in milliseconds of various cryptographic operations for the three schemes. The cryptographic schemes were tested on various standard quality reports of variable sizes. It can be noticed that the ECCDSA takes less time compared to the RSADSA. This is expected because of the ability of the ECC to provide the required level of security using much smaller key sizes. Therefore, the current research adopts the ECCDSA as the standard algorithm to provide non-repudiation and authentication services. In addition, the AES algorithm was implemented to provide confidentiality. The experimental results showed that the ECIES algorithm takes a longer time compared to other algorithms. This is perhaps due to the need to exchange keys and generate an HMAC. The algorithm does not provide a non-repudiation service, which is required for many quality transactions. Therefore, it is not recommended for the current quality system implementation.

Table 3. Time consumption results for the cryptographic operations.

Quality Reports	Size (Kilobytes)	Time Consumption of AES_ECCDSA Cryptographic Operations		Time Consumption of AES_RSADSA Cryptographic Operations		Time Consumption of ECIES Cryptographic Operations
		AES	ECCDSA	AES	RSADSA	HMAC and Encryption
Quality Contracts	447 KB	3	33	2	40	150
Course Reports	1215 KB	43	64	43	81	282
Annual Program Report	8088 KB	**57**	131	**57**	174	739
Course Specification	597 KB	14	54	14	69	218
Program Specification	1167 KB	18	58	18	86	227

Figure 10 shows a comparison in terms of the total time consumed by the digital signature and encryption operations of the ECCDSA and RSADSA and the total time consumed by ECIES operations. It can be noticed that the ECCDSA achieved the best results, followed by the RSA. However, the ECIES algorithm took a longer time to execute in comparison to other cryptographic schemes.

Table 4 presents the time consumption (in seconds) results for different cryptographic operations with blockchain transactions for data sizes ranging from 400 to 1200 KB. It is evident that the AES_ECCDSA hybrid cryptographic scheme consistently performs the best compared to other schemes. This is expected, as the time consumption of blockchain transactions is directly related to the file size, regardless of the cryptographic algorithm used. The lowest time consumption was observed when using the AES_ECCDSA for encrypting, signing, and storing a file of approximately 400 KB. In contrast, the ECIES scheme resulted in the longest processing time for files compared to other algorithms.

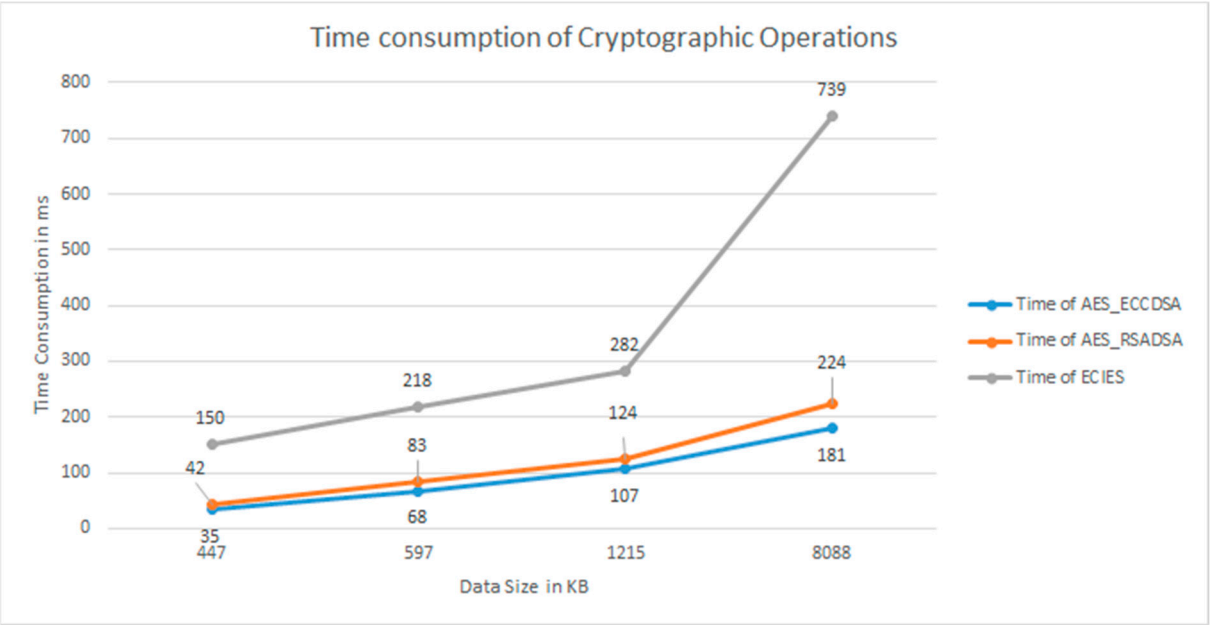


Figure 10. Time consumption of different cryptographic schemes.

Table 4. Time consumption results for the cryptographic operations with blockchain transactions.

Data Size (Kilobytes)	Time Consumption of Cryptographic Schemes with Blockchain		
	AES_ECCDSA	AES_RSADSA	ECIES
400 KB	30.036	30.42	30.150
800 KB	60.107	60.124	60.282
1200 KB	90.188	90.231	90.739

The following discussion highlights the advantages of utilizing the proposed blockchain-based ecosystem from a security perspective.

4.3. Features of the Proposed Blockchain-Based QAS

This section explains how the blockchain technology, through its powerful security features, can improve privacy and provide secure and trustworthy environment for the QAS. Additionally, the discussion clarifies the improvements in efficiency of various quality operations that can be achieved by implementing blockchain and smart contracts.

4.3.1. Privacy

Ensuring the protection of users' privacy is a crucial aspect of a QAS. As the quality assurance and accreditation processes involve sensitive transactions and decision-making, it is imperative to provide privacy to various users, including independent reviewers and quality members. The blockchain's anonymity feature can enhance user privacy by concealing personal information on the platform. Users can conduct transactions through their blockchain wallet, with each user being identified by their public key. For instance, the personal details of independent reviewers who are responsible for assessing a program's eligibility for accreditation are not visible to quality members or program representatives. This is akin to the blind peer review process used by scholarly journals for research articles.

4.3.2. Integrity

QAPs generate crucial information and reports that contribute towards decision-making and continuous improvement planning. Therefore, it is imperative to maintain the integrity of quality-related information and never compromise it. Blockchain's immunity

feature, which is powered by cryptographic algorithms, is the cornerstone of providing integrity services in the QAS. Quality reports and transactions saved in the blockchain cannot be tampered with, ensuring the authenticity and reliability of sensitive quality information. The proposed quality assurance ecosystem has adopted the IPFS technology to overcome the storage limitations of blockchain. Quality documents are stored offline using the IPFS, while only the hash codes are stored online in the blockchain platform. This saves storage space and enhances the performance of blockchain transactions.

4.3.3. Accountability and Transparency

Blockchain technology is a powerful tool that brings transparency and accountability to transactions within the QAS. With the use of private keys, users can approve quality reports, sign smart contracts, and take responsibility for their actions. By utilizing public key encryption, users can trust that their signed contracts are legitimate and approved by the intended parties. The beauty of this blockchain-based ecosystem is that it offers accountability without sacrificing privacy. While users are accountable for all transactions within their blockchain wallet, their personal information is only visible to higher authorities. This ensures the safety and confidentiality of user information while promoting transparency and trust within the quality assurance ecosystem.

4.3.4. Traceability

The proposed quality assurance platform leverages the power of blockchain technology to include a traceability feature. This state-of-the-art platform allows for streamlined tracking of all QAS transactions, providing all involved parties with the ability to verify the timeline of quality assurance activities. This aspect of the QAS is essential, as it bolsters the credibility of the entire environment and ensures that quality assurance activities are completed in a timely fashion. With this level of transparency, stakeholders can make informed decisions efficiently and effectively.

4.3.5. Efficiency

Within the current blockchain-based ecosystem, smart contract technology is utilized to enhance the efficiency of quality assurance transactions. These transactions are automated and can be processed much faster than manual QAS processes. For instance, once the HEI representative signs the smart contract, the request for evaluation is automatically transmitted to the accreditation authority. Similarly, when quality members approve a particular quality report by signing the corresponding smart contract, the subsequent quality assurance procedure is automatically triggered at a higher level of authority. This streamlines quality processes, saving time and effort and ensuring promptness.

Moreover, by employing smart contracts, the need for a third party to oversee QAPs is avoided, as all transactions are automated and transparent. This reduces the workload for all parties involved in the QAS and conserves valuable resources.

5. Conclusions and Future Work

A QAS is crucial for academic programs in HEIs. It processes sensitive information that is integral to decision-making and improvement planning. However, traditional QASs face several cybersecurity challenges, including issues related to privacy, reliability, integrity, and trustworthiness. Furthermore, current QASs lack effective governance, which represents a significant challenge that must be addressed to ensure the efficiency and reliability of quality assurance operations.

This study proposes a blockchain-based QAS to improve the security of information assets and enhance the governance of quality processes for academic programs. The current approach employs Ethereum blockchain, along with an authentication and authorization layer that controls access to system resources. Smart contract technology is utilized to perform transactions and enhance the efficiency of the QAS. This study also presents a prototype implementation of the blockchain-based QAS, which includes essential processes,

such as processing and approving quality reports at the departmental and institutional levels, independent reviews, and program accreditation processes. The blockchain-based platform successfully provides a secure and trustworthy quality ecosystem, supported by valuable security services, ensuring qualities such as integrity, accountability, transparency, and traceability. Additionally, the current blockchain platform enhances the privacy of users, which is crucial for sensitive processes, such as independent reviews.

Furthermore, the current study leverages a hybrid cryptographic scheme to ensure that the application layer is secure. The experimental results showed that the ECCDSA coupled with AES encryption provides better performance than other cryptographic algorithms, resulting in a reduced time delay.

Future research will extend the blockchain-based QAS to include important processes related to institutional accreditation. Additionally, future studies will investigate the adaptation of various blockchain platforms and consensus algorithms to improve the performance and reduce the transactional costs.

Author Contributions: Conceptualization, M.A.; methodology, F.S.; software, M.A.; validation, F.S.; investigation, M.A.; resources, T.A.; writing—original draft preparation, M.A.; writing—review and editing, T.A.; visualization, F.S.; supervision, M.A.; project administration, M.A.; funding acquisition, M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-RPP2023012).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

Notation	Description
QAS	Quality assurance system
DDoS	Denial-of-Service Attacks
DSA	Digital signature algorithm
dApps	Decentralized applications
IPFS	Interplanetary file system
ECCDSA	Elliptic curve cryptography DSA
RSADSA	RSA digital signature
ECIES	Elliptic Curve Integrated Encryption Scheme

References

1. Shafi, A.; Saeed, S.; Bamarouf, Y.A.; Iqbal, S.Z.; Min-Allah, N.; Alqahtani, M.A. Student Outcomes Assessment Methodology for ABET Accreditation: A Case Study of Computer Science and Computer Information Systems Programs. *IEEE Access* **2019**, *7*, 13653–13667. [CrossRef]
2. Sanjaya, M. *Quality Assurance in Higher Education: An Introduction*; National Assessment and Accreditation Council: Bangalore, India, 2007.
3. Ryan, T. Quality assurance in higher education: A review of literature. *High. Learn. Res. Commun.* **2015**, *5*. [CrossRef]
4. Cojocariu, A.-C.; Verzea, I.; Chaib, R. Aspects of Cyber-Security in Higher Education Institutions. In *Innovation in Sustainable Management and Entrepreneurship, Proceedings of the 2019 International Symposium in Management (SIM2019), Timisoara, Romania, 25–26 October 2019*; Springer: Berlin/Heidelberg, Germany, 2020.
5. Mello, S. Data Breaches in Higher Education Institutions. Bachelor's Thesis, University of New Hampshire, Durham, NH, USA, 2018.
6. Edwards, M.A.; Roy, S. Academic research in the 21st century: Maintaining scientific integrity in a climate of perverse incentives and hypercompetition. *Environ. Eng. Sci.* **2017**, *34*, 51–61. [CrossRef]
7. Flanagan, B.; Ogata, H. Integration of learning analytics research and production systems while protecting privacy. In Proceedings of the 25th International Conference on Computers in Education, Christchurch, New Zealand, 4–8 December 2017.

8. Tierney, R.D. *Fairness in Educational Testing and Assessment*; Routledge: London, UK, 2022.
9. Mohammad, A. An Effective and Secure Quality Assurance System for a Computer Science Program. *Comput. Syst. Sci. Eng.* **2022**, *41*, 975–995.
10. Chan, W.W. International cooperation in higher education: Theory and practice. *J. Stud. Int. Educ.* **2004**, *8*, 32–55. [CrossRef]
11. Matzutt, R.; Müllmann, D.; Zeissig, E.M.; Horst, C.; Kasugai, K.; Lidynia, S.; Ziefle, M. *myneData: Towards a Trusted and User-Controlled Ecosystem for Sharing Personal Data*; INFORMATIK 2017; Gesellschaft für Informatik: Bonn, Germany, 2017.
12. Andrew, J.; Isravel, D.P.; Sagayam, K.M.; Bhushan, B.; Sei, Y.; Eunice, J. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *J. Netw. Comput. Appl.* **2023**, *215*, 103633.
13. Silva, S.; Pires, F.; Bernardino, J. Editorial platform in blockchain for application in higher education. In Proceedings of the ICETE 2019—16th International Joint Conference on e-Business and Telecommunications, Prague, Czech Republic, 26–28 July 2019; Volume 1, pp. 221–227.
14. Arndt, T.; Guercio, A. Blockchain-based transcripts for mobile higher-education. *Int. J. Inf. Educ. Technol.* **2020**, *10*, 84–89. [CrossRef]
15. Lizcano, D.; Lara, J.A.; White, B.; Aljawarneh, S. Blockchain-based approachto create a model of trust in open and ubiquitous higher education. *J. Comput. High Educ.* **2020**, *32*, 109–134. [CrossRef]
16. Sharples, M.; Domingue, J. The Blockchain and Kudos: Adistributed system for educational record, reputation and reward. In *EC-TEL 2016: Adaptive and Adaptable Learning, Proceedings of the 11th European Conference on Technology Enhanced Learning, EC-TEL 2016, Lyon, France, 13–16 September 2016*; Verbert, K., Sharples, M., Klobučar, T., Eds.; Springer: Cham, Switzerland, 2016.
17. Matzutt, R.; Pennekamp, J.; Wehrle, K. A secure and practical decentralized ecosystem for shareable education material. In Proceedings of the 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 7–10 January 2020; IEEE: Piscataway, NJ, USA, 2020.
18. Palma, L.M.; Vigil, M.A.G.; Pereira, F.L.; Martina, J.E. Blockchain and smart contracts for higher education registry in Brazil. *Int. J. Netw. Manag.* **2019**, *29*, e2061. [CrossRef]
19. Ricardo, R.; Rosário, A. Blockchain system in the higher education. *Eur. J. Investig. Health Psychol. Educ.* **2021**, *11*, 276–293.
20. Benet, J. IPFS—Content Addressed, Versioned, P2P File System. *arXiv* **2014**, arXiv:1407.3561.
21. He, X. An overview of the decentralized storage technology and its applications. *J. Phys. Conf. Ser.* **2018**, *1087*, 062017.
22. Martin, T. Reflections on the transition from elite to mass to universal access: Forms and phases of higher education in modern societies since WWII. In *International Handbook of Higher Education*; Springer: Dordrecht, The Netherlands, 2007; pp. 243–280.
23. Fincher, S.; Kölling, M.; Utting, I.; Brown, N.; Stevens, P. Repositories of teaching material and communities of use: Nifty assignments and the greenroom. In Proceedings of the Sixth International Workshop on Computing Education Research, Aarhus, Denmark, 9–10 August 2010.
24. Henze, M.; Wolters, B.; Matzutt, R.; Zimmermann, T.; Wehrle, K. Distributed configuration, authorization and management in the cloud-based internet of things. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, Australia, 1–4 August 2017; IEEE: Piscataway, NJ, USA, 2017.
25. Datta, P.K.; Mitra, S. Application of Blockchain in Online Learning: Findings in Higher Education Certification. In *The Data-Driven Blockchain Ecosystem*; CRC Press: Boca Raton, FL, USA, 2022; pp. 103–111.
26. Ocheja, P.; Flanagan, B.; Ueda, H.; Ogata, H. Managing lifelong learning records through blockchain. *Res. Pract. Technol. Enhanc. Learn.* **2019**, *14*, 4. [CrossRef]
27. Cardoso, S.; Mamede, H.S.; Santos, V. Reference model for academic results certification in student mobility scenarios: Position paper. In Proceedings of the 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Sevilla, Spain, 24–27 June 2020; IEEE: Piscataway, NJ, USA, 2020.
28. Awaji, B.; Solaiman, E.; Marshall, L. Investigating the requirements for building a blockchain-based achievement record system. In Proceedings of the 5th International Conference on Information and Education Innovations, London, UK, 26–28 July 2020.
29. Lam, T.Y.; Dongol, B. A blockchain-enabled e-learning platform. *Interact. Learn. Environ.* **2022**, *30*, 1229–1251. [CrossRef]
30. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; IEEE: Piscataway, NJ, USA, 2015.
31. Karamitsos, I.; Papadaki, M.; Al-Hussaeni, K.; Kanavos, A. Transforming Airport Security: Enhancing Efficiency through Blockchain Smart Contracts. *Electronics* **2023**, *12*, 4492. [CrossRef]
32. Gerardi, M.; Fallucchi, F.; Orecchini, F. Blockchain Technology for Monitoring Energy Production for Reliable and Secure Big Data. *Electronics* **2023**, *12*, 4660. [CrossRef]
33. Satoshi, N. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 14 April 2024).
34. Haifa, A.; Alkhatib, M. Towards improving privacy and security of identity management systems using blockchain technology: A systematic review. *Appl. Sci.* **2022**, *12*, 12415. [CrossRef]
35. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. White Paper 3.37 (2014): 2-1. Available online: https://finpedia.vn/wp-content/uploads/2022/02/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed on 20 April 2024).
36. Narayan, P. *Blockchain for Enterprise: Build Scalable Blockchain Applications with Privacy, Interoperability, and Permissioned Features*; Packt Publishing Ltd.: Birmingham, UK, 2018.

37. AlKhatib, M. Smart Contract Code, Source Code, Version 1.0, 2024. M. AlKhatib, in AES_ECC Cryptographic Scheme Code, Source Code, Version 1.0. 2024. Available online: https://drive.google.com/drive/folders/1yn75uw0YUISNM0nR2RGd2Vr9y0szZBkp (accessed on 10 April 2024).
38. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32. Available online: https://www.scirp.org/reference/referencespapers?referenceid=2723155 (accessed on 10 March 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.